PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-324419
(43)Date of publication of application : 14.11.2003

(51)Int.Cl. H04L 9/08
H04Q 7/38

(21)Application number : 2003-041758
(22)Date of filing : 19.02.2003

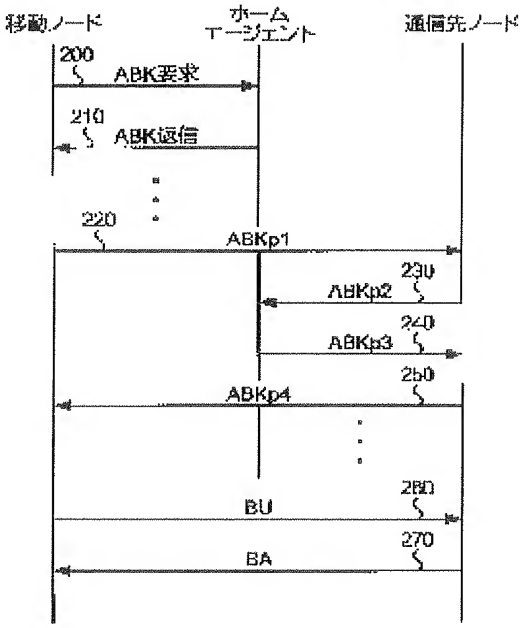
(71)Applicant : DOCOMO COMMUNICATIONS LABORATORIES USA INC
(72)Inventor : KEMPF JAMES
DESAI ANAND
OKAZAKI SATOMI
YIN YIQUN LISA
GENTRY CRAIG
SILVERBERG ALICE

(30)Priority

Priority number	Priority date	Priority country
2002 358177	19.02.2002	US
2002 416029	03.10.2002	US
2003 364289	11.02.2003	US

(54) METHOD OF SECURING BINDING UPDATE BY USING ADDRESS BASED KEY

(57)Abstract:
PROBLEM TO BE SOLVED: To secure binding updates in a wireless telecommunications system.
SOLUTION: A public key is generated by using a home address of a mobile host. A home agent, such as a router, generates a private key by using public cryptographic parameters corresponding to the mobile host or the public key. A node of a communication destination uses the public key to encrypt a shared key and sends the encrypted shared key to the mobile host. The mobile host decrypts the shared key by using its original private key. The shared key is used for signing the binding update. Thereafter, the node of the communication destination utilizes the shared key to verify the authenticity of the binding update.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－324419
（P2003－324419A）
(43)公開日　平成15年11月14日(2003.11.14)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｄ	５Ｊ１０４
Ｈ０４Ｑ　7/38			６０１Ｅ	５Ｋ０６７
		Ｈ０４Ｂ　7/26	１０９Ｒ	

審査請求　未請求　請求項の数26　ＯＬ　外国語出願　（全 48 頁）

(21)出願番号　特願2003－41758(P2003－41758)

(22)出願日　平成15年２月19日(2003.2.19)

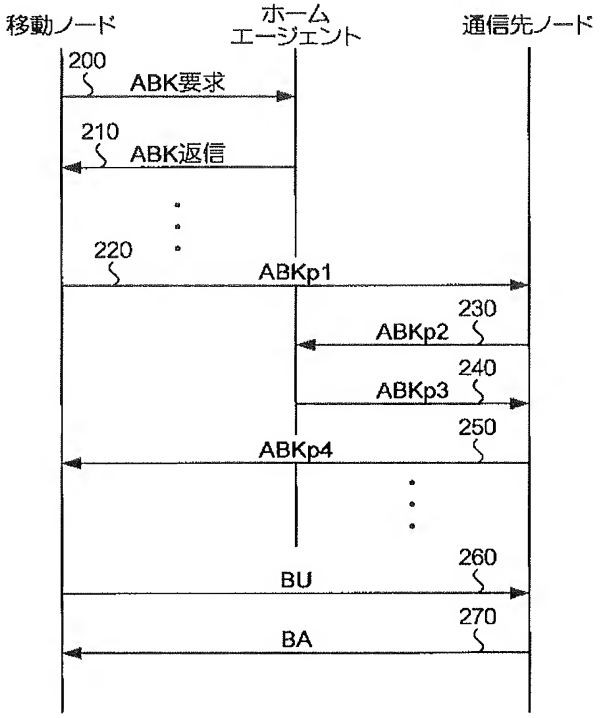
(31)優先権主張番号　６０／３５８１７７
(32)優先日　平成14年２月19日(2002.2.19)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　６０／４１６０２９
(32)優先日　平成14年10月３日(2002.10.3)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　１０／３６４２８９
(32)優先日　平成15年２月11日(2003.2.11)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　301077091
ドコモ　コミュニケーションズ　ラボラトリーズ　ユー・エス・エー　インコーポレーティッド
アメリカ合衆国，カリフォルニア州　95110，サンノゼ，スイート300，メトロドライブ　181
(74)代理人　100098084
弁理士　川▲崎▼　研二　（外１名）

最終頁に続く

(54)【発明の名称】　アドレス・ベースド・キーを使用して対応情報更新を保護する方法

(57)【要約】
【課題】　無線通信システム内で対応情報更新を保護する。
【解決手段】　移動ホストのホームアドレスを使用して、公開鍵が生成される。ルータ等のホームエージェントは、移動ホストまたは公開鍵に対応した、公開暗号パラメータを用いて秘密鍵を生成する。通信先ノードは、公開鍵を使って共有鍵を暗号化する。そして、暗号化された共有鍵を移動ホストに届ける。移動ホストは、独自の秘密鍵を使用して共有鍵を復号化する。この共有鍵は対応情報更新を署名するために用いられる。以後、対応情報更新を認証するために、通信先ノードは共有鍵を利用する。



1

【特許請求の範囲】

【請求項１】　無線通信システムで対応情報更新を保護する方法であり、
公開識別子を使用して公開鍵を生成するステップと、
前記公開鍵を使用して秘密鍵を生成するステップと、
前記公開鍵および前記秘密鍵を利用して対応情報更新を保護するステップとを備えることを特徴とする方法。

【請求項２】　ホームエージェントは前記公開鍵を生成することを特徴とする請求項１に記載の方法。

【請求項３】　ホームエージェントは前記秘密鍵を生成することを特徴とする請求項１に記載の方法。

【請求項４】　前記ホームエージェントは、前記秘密鍵を前記移動ホストに提供することを特徴とする請求項３に記載の方法。

【請求項５】　前記公開鍵と、共有鍵と、公開パラメータを使用して、移動ホストとの間で伝達される対応情報更新を保護する、前記移動ホストに接続可能な通信先ノードをさらに備えることを特徴とする請求項４に記載の方法。

【請求項６】　前記通信先ノードは、前記公開鍵と前記公開パラメータを使用して、前記共有鍵を暗号化することを特徴とする請求項５に記載の方法。

【請求項７】　前記移動ホストは前記共有鍵を使用して前記対応情報更新を署名し、この対応情報更新を前記通信先ノードに送信することを特徴とする請求項５に記載の方法。

【請求項８】　前記ホームエージェントは、前記公開パラメータを前記通信先ノードに提供することを特徴とする請求項５に記載の方法。

【請求項９】　前記移動ホストのホームアドレスを使用して前記公開鍵が生成されることを特徴とする請求項１に記載の方法。

【請求項１０】　無線通信システムでの対応情報更新を保護するシステムであって、
前記通信システムに接続可能な移動ホストと、
公開鍵と秘密鍵を使用して、移動ホストとの間で伝達される対応情報更新を保護する、前記移動ホストに接続可能な通信先ノードとを備えることを特徴とするシステム。

【請求項１１】　前記移動ホストと通信先ノードに接続可能なホームエージェントをさらに備えることを特徴とする請求項１０に記載のシステム。

【請求項１２】　前記ホームエージェントは、前記秘密鍵と公開パラメータを生成することを特徴とする請求項１１に記載のシステム。

【請求項１３】　前記移動ホストのホームアドレスを使用して前記公開鍵が生成されることを特徴とする請求項１０に記載のシステム。

【請求項１４】　前記ホームエージェントは前記秘密鍵を生成することを特徴とする請求項１１に記載のシステム。

2

【請求項１５】　前記ホームエージェントは、前記秘密鍵と公開パラメータを前記移動ホストに提供することを特徴とする請求項１１に記載のシステム。

【請求項１６】　通信先ノードは、前記公開鍵および公開パラメータを用いて、共有鍵を暗号化することを特徴とする請求項１５に記載のシステム。

【請求項１７】　前記移動ホストは前記共有鍵を使用して前記対応情報更新を署名し、この対応情報更新を前記通信先ノードに伝達することを特徴とする請求項１６に記載のシステム。

【請求項１８】　前記移動ホストは、前記公開パラメータを前記通信先ノードに提供することを特徴とする請求項１６に記載のシステム。

【請求項１９】　無線通信システムで使用され、
前記通信先ノードとの間で伝達される対応交信情報を保護するために、公開鍵および秘密鍵が使用される、自身をホームエージェントと通信先ノードに接続することが可能なインターフェースを有することを特徴とする移動ノード。

【請求項２０】　前記ホームエージェントは、前記秘密鍵と公開パラメータを生成することを特徴とする請求項１９に記載の移動ノード。

【請求項２１】　前記公開鍵は、前記移動ノードのホームアドレスを使って生成されることを特徴とする請求項１９に記載の移動ノード。

【請求項２２】　前記ホームエージェントは前記秘密鍵を生成することを特徴とする請求項１９に記載の移動ノード。

【請求項２３】　前記ホームエージェントは、前記秘密鍵および公開パラメータを前記移動ノードに提供することことを特徴とする請求項１９に記載の移動ノード。

【請求項２４】　前記通信先ノードは、前記公開鍵と前記公開パラメータを使って共有鍵を暗号化することを特徴とする請求項２３に記載の移動ノード。

【請求項２５】　前記移動ノードは、前記共有鍵を使用して前記対応情報更新を署名し、前記対応情報更新を前記通信先ノードに送信することを特徴とする請求項２４に記載の移動ノード。

【請求項２６】　前記公開パラメータを前記通信先ノードに提供するために、前記インターフェースが使用されることを特徴とする請求項２４に記載の移動ノード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、個別暗号化システムに関し、特に、無線通信システム内での対応情報更新を保護するための方法およびシステムに関する。

【０００２】

【従来の技術】本願は、仮米国特許出願番号６０／３５８，１７７（２００２年２月１９日出願）と６０／４１

６，０２９（２００２年１０月３日出願）に基づいて優先権主張する。なお、これらは「アドレス・ベースド・キーを使ったＭＩＰｖ６対応情報更新（Ｂｉｎｄｉｎｇ　Ｕｐｄａｔｅ）の保護」との名称を付されており本文中でも参照した。

【０００３】よく知られたモバイルＩＰ様式の研究と、ＭＩＰｖ６対応情報更新を保護する基本技術の成果として、往復経路確認（Ｒｅｔｕｒｎ　Ｒｏｕｔａｂｉｌｉｔｙ）を受け入れるか否かの技術的議論の風潮が本発明の背景にある。今日、往復経路確認に関して発案された様々な機構が存在する。しかし往復経路確認には、その保護特性とパフォーマンスに関して問題がある。

【０００４】

【発明が解決しようとする課題】暗号化社会においては、個別暗号化システムが知られているが、そうしたシステムはネットワーキング保護対策では利用されていない。最新のネットワーキング保護対策には、ディフィ・ヘルマン技術が利用されている。また最近まで、暗号化に利用可能な個別暗号化アルゴリズムは存在しなかった。従来型アルゴリズムは電子署名のみ扱っており、その技術範囲は限られたものであった。最新の研究では、暗号化を同様に可能にする、楕円曲線に基づいた新しいアルゴリズムを提示する。

【０００５】

【課題を解決するための手段】本発明は、無線通信システムでの対応情報更新を保護するためのシステムおよび方法を開示する。本システムでは、移動ホストのホームアドレスを利用して公開鍵が作られる。そしてホームエージェントは、移動ホストと公開鍵に対応した、公開暗号パラメータを利用して秘密鍵を作る。

【０００６】通信先ノードと通信を開始する場合、移動ホストは、通信先ノードがホームエージェントから公開暗号パラメータを取得するように要求するメッセージを、ホームエージェントを通じて、通信先ノードに伝送する。ここで、通信先ノードが暗号パラメータを有していない場合、通信先ノードはホームエージェントから暗号パラメータを取得する。次に通信先ノードは、移動ホストのホームアドレスと、暗号パラメータを利用して、ホームエージェントを介して移動ホストに送信される共有鍵を暗号化する。移動ホストは公開鍵を利用して、受け取った共有鍵を復号化するとともに、この共有鍵を使用して、対応情報更新に含まれたメッセージ認証コードを算出する。この処理を受けて通信先ノードは、共用秘密鍵を使用してメッセージ認証コードを検査することによって、対応情報更新を保護する。

【０００７】

【発明の実施の形態】以下、図面を参照して、通信対応情報更新を保護するための機構における好ましい実施形態について記載する。なお、同一の構成要素は同一の番号によって識別されるものとする。かかる保護機構は、アドレス・ベースド・キー（ＡＢＫ）、またはウェール・ペアリングと、秘密暗号化方式の組み合わせに基づいた暗号システムとを参照した他の暗号化方法を含んでいる。以下の記載は、本発明が有する性質の一態様を示すことを目的としており、その技術的思想の範囲を限定するものではない。

【０００８】個人の識別子をベースとした暗号化（以下、個別暗号化という）を利用した、ＭＩＰｖ６での対応情報更新を保護するためのシステムおよび方法について説明する。個別暗号化は、クライアントが、そのＩＰアドレス等、当該クライアントの公開識別子を公開鍵として利用する、一連の暗号手法を含む。クライアントは、公開暗号パラメータとともに、秘密鍵を個別秘密鍵生成部（ＩＰＫＧ）から取得する。メッセージを暗号化する必要がある通信相手先は、そのメッセージの宛先であるクライアントの公開ＩＤと公開暗号パラメータを使用する。さらに通信相手先は、ＩＰＫＧから公開暗号パラメータを取得する。クライアントは、当該クライアントの秘密鍵によって、暗号化されたメッセージを復号化する。

【０００９】図１は、無線モバイルアクセスＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）ネットワークの一例を示す。無線モバイルアクセスＩＰネットワークは、多数の固定ノード（すなわち、固定接続ポイントまたは固定接続網）から構成される、固定ノードＩＰデータネットワーク１２０を含む。このネットワークではデータは、本明細書の参考文献であるＩＥＴＦ　ＲＦＣ　２４６０として指定されたＩＰｖ６等のインターネットプロトコルに従って流れる。コアネットワーク１２０には、ＩＰモバイルバックボーン１４０を形成する多数のゲートルータ１３０の集まりが設けられており、このルータ群は、従来のインターネット・アドレッシングプロトコルおよびインターネット・ルーティングプロトコルに従って機能することにより、コアネットワークに接続された送信元ノードと宛先ノードとの間でデータパケットをルーティングする。ＩＰモバイルバックボーン１４０を形成する個々のゲートルータ１３０は、それら自体がコアネットワーク１２０に接続されたノードであり、また、コアネットワーク１２０内で通信するための独自のアドレスを有する。

【００１０】ゲートルータ１３０の各々には、サーバもしくはルータ１４５が接続されており、これらはユニークなＩＰアドレスを有し、移動ノード１３５のような移動ホストと通信先ノード１４２をコアネットワーク１２０にインターフェースするホームエージェント（ＨＡ）としての機能を備えている。移動ノード１３５は、通信先ノード１４２と通信を行うためのインターフェースを有している。同様に、通信先ノードの側も、移動ノードと通信を行うためのインターフェースを有している。なお、通信先ノード１４２が、移動ノードである場合もあ

る。移動ノード１３５と通信先ノード１４２は、それぞれ、携帯ハンドセット、携帯電話、携帯型コンピュータ、パーソナル情報マネージャ、および無線データ端末等、各種の無線移動装置を含み得る。

【００１１】移動ノード１３５は、ホームリンク上の1つ以上のホームエージェント１４５との間でセキュリティ・アソシエーションを確立している。そして移動ノード１３５は、ネットワーク１００内の異なる接続ポイント間の移動を検知するようにプログラミングされている。移動ノード１３５は、ホームアドレス、すなわち、移動ノード１３５自身がネットワーク１００内を移動しても変化しない移動ノード１３５のアドレスによって特定されうる。さらに移動ノード１３５は、ネットワーク１００内で訪れた各地点での一時的な気付アドレス（Ｃａｒｅ　Ｏｆ　Ａｄｄｒｅｓｓ；ＣＯＡ）を取得する。また移動ノード１３５は、ＩＰｓｅｃセキュリティ・アソシエーションによって保護された対応情報更新メッセージを送出することで、ホームエージェントに気付アドレス変更を通知する。

【００１２】ホームエージェントおよびフォーリンエージェント１４５は、移動ノード１３５と通信先ノード１４２がホームエージェントおよびフォーリンエージェントと通信を行うための、無線アクセスネットワーク１５０を有する。ホームエージェント１４５は、移動ノード１３５の所在位置を追跡記録して、移動ノード１３５へ（ある実施形態では、移動ノードから）パケットを転送する、ホームリンクのルータとともに備えられても良い。なお、ホームエージェントアドレス（ＨＡＡ）は、ホームエージェント１４５のネットワークアドレスを指す。

【００１３】無線アクセスネットワーク１５０は、複数の無線アクセスポイント１５５を含むものでもよい。なお、無線アクセスネットワークの構造、設置、および機能は従来型でありかつ標準的なものとする。無線ＬＡＮまたはデジタル通信技術は、複数の無線型移動ノード１３５および無線アクセスポイントで、通常の方法によって実行される。この点に関する詳細は、本発明の完全な理解かつ認識に必ずしも必要ではないので、その説明を以下では省略する。

【００１４】通信での対応情報更新を保護する機構では、移動ノード１３５と多数のホームエージェント１４５との間における通信保護を一層確実にするために、アドレス・ベースド・キーを使用する。このアドレス・ベースド・キーは、個別暗号化システムでの長期結果を利用して、移動ノード１３５のＩＰアドレスに基づく公開鍵を作る。

【００１５】セキュリティ・アソシエーションは、ftp://ftp.isi.edu/in-notes/rfc2401.txtに示されたＩＰセキュリティ・プロトコルによって、移動ノード１３５とホームエージェント１４５の間に設立される。セキュリティ・アソシエーションによって、暗号化パラメータ情報が、極秘かつ認証化されて移動ノード１３５へ伝達される。移動ノード１３５、ホームエージェント１４５、および通信先ノード１４２は個別暗号化システムを構成する。ホームエージェント１４５は、個別秘密鍵生成部（以下、ＩＰＫＧ）、もしくはＩＰＫＧへの安全なアクセス手段を備える。

【００１６】移動ノード１３５は好ましくは、ホームリンク上の１または複数のホームエージェント１４５との間でセキュリティ・アソシエーションを確立したノードである。ホームリンクは、移動ノードのホームアドレスが位相的に配置された、移動ノードのホームネットワーク内でのサブネットを含む。移動ノード１３５は、ネットワーク１００内の異なる接続ポイント間の移動をそれ自身が検知することが可能である。移動ノード１３５は、ネットワーク１００内の移動先において一時的な気付アドレスを取得することができ、セキュリティ・アソシエーションを利用して、現在保持している気付アドレスをホームエージェント１４５に通知する。通信先ノード１４２は、移動ノード１３５が通信する相手先ノードを指す。通信先ノードは、移動性であってもよい。移動ノード１３５は、それ自身がネットワーク内１００を移動しても変化しない、移動ノードのアドレスを含んだホームアドレス（ＨｏＡ）を有する。ホームエージェントは、ホームアドレスを割り当てて移動ノード１３５に送信することができる。

【００１７】ホームエージェント１４５は、ホームリンク上のルータに実装されてもよい。このホームエージェント１４５は、移動ノードの現在地を逐一把握して、移動ノード１３５へ（ある実施形態では、移動ノードから）パケットを転送するために使用される。移動ノードの現在地を特定するために、気付アドレス（ＣｏＡ）ＩＰアドレスが移動ノード１３５に割り当てられる。移動ノード１３５は、ホームエージェントを介したパケットのルーティングを回避するため、通信先ノード１４２との間でルート最適化を実行しても良い。ルート最適化によって、移動ノード１３５と通信先ノード１４２の間の通信のレーテンシを少なくすることができる。移動ノード１３５は、その気付アドレスが変更されると、通信先ノード１４２に対応情報更新を伝達することによりルート最適化を実行する。アドレス・ベースド・キーは、移動ノード１３５と通信先ノード１４２が、かかる対応情報更新の正当性を確認することを可能にする技術である。

【００１８】アドレス・ベースド・キー暗号化技術は、移動ノードのホームアドレスを利用してその公開鍵を生成するための、個別暗号化システムを採用する。また個別暗号化システムには、認証、暗号鍵使用取り決め、および暗号化における公開鍵として、ＩＰｖ６アドレス等の良く知られた識別子を利用したシステムがある。個別

秘密鍵生成部（ＩＰＫＧ）は、コンピュータ・プロセッサ等のエージェントを含む。このコンピュータ・プロセッサは、公開鍵として機能する公開識別子を受け取ると、個別暗号化アルゴリズムを実行して秘密鍵を作る。

【００１９】個別暗号化システムでは、ノードのｅメールアドレスやＩＰアドレス等の一般に知られた識別子は、電子認証演算、暗号鍵使用取り決め、および暗号化に用いる、公開鍵／秘密鍵の組み合わせにおける公開鍵として機能する。個別署名プロトコルでは、ホスト、すなわち、移動ノード１３５は、ＩＰＫＧによって供給された秘密鍵を使用してメッセージに署名する。すると、ホストの識別子を利用してこの署名が認証される。個別暗号化では、暗号化する側はメッセージを受領する側の公開識別子を利用してメッセージを暗号化する。メッセージ受領者は、その受領者の秘密鍵によって暗号化された暗号文を解読する。公開鍵暗号化では一般的であるが、暗号化システムのセキュリティは、ファクタリングや個別ログ（あるいは、ディフィ・ヒルマン）問題等、その具体的数字理論問題が解決される難易度によって異なる。個別暗号化システムは、鍵供託（キーエスクロー）を利用して、あるいは利用することなく解釈される。鍵供託を利用するプロトコルは、鍵供託を利用しないプロトコルよりも少ないパスによって実行されうる。分散生成方法を応用した技術によって、多数のＩＰＫＧ間でマスター鍵情報が分散もしくは共有されることから、ホストの秘密鍵を知るためにすべてのＩＰＫＧが結託することが可能である。そのようなシナリオは、必要な場合、すべてのＩＰＫＧが合意することによって鍵供託方式を採用する余地を生じさせる。この結果、相互の合意なしに、秘密鍵に関する情報がＩＰＫＧによって保護される。

【００２０】個別暗号化システムは、認証、暗号鍵使用取り決め、および暗号化に使用される公開鍵として、ＩＰｖ６等の良く知られた識別子を利用可能な暗号システムを含む。アドレス・ベースド・キーは、公開暗号化パラメータを用いて移動ノードの公開鍵と秘密鍵を作るために、個別暗号化システムを導入した暗号化技術のことである。個別キーには、楕円曲線アルゴリズムを実装するのが好ましい。なぜなら、楕円曲線アルゴリズムは小さなキーに良く適合し、小規模な無線装置等の小規模ホストでの演算を効率的にし、また、より小さな署名を生成するからである。楕円曲線の代わりにアーベル多様体を使用することによって、非楕円曲線アルゴリズム等、異なるタイプのアルゴリズムが個別キーに実装されても良い。

【００２１】公開暗号パラメータは、公開された様々なパラメータを含む。これら様々なパラメータは、ＩＰＫＧ（個別秘密鍵生成部）のみに知られた、定数と秘密マスターキーによって形成された、個別暗号化アルゴリズムに特定なパラメータのことである。ＩＰＫＧは、公開鍵として機能する公開識別子を提供されると、秘密鍵を作るために個別暗号化アルゴリズムを実行するエージェントを含む。好ましい公開識別子は、移動ノードのホームアドレス（ＨｏＡ）を含む。ＩＰＫＧは、秘密マスターキーを使用して秘密鍵を作るとともに、移動ノード１３５と通信先ノード１４２に提供される、公開暗号パラメータを作成する。秘密マスターキーによって生成される公開暗号パラメータは、メッセージの保護もしくは暗号化の各動作に関与する、移動ノード１３５と通信先ノード１４２等、ノード間の暗号化処理に用いられる。

【００２２】図２は、対応情報更新を保護するための、個別暗号化システムの使用法を示すラダー図である。移動ノード１３５は、公開識別子を、ＩＰＫＧとして機能するホームエージェント１４５に送る（ブロック２００）。公開識別子は、移動ノード１３５のホームアドレス（ＨｏＡ）を含む。移動ノードの公開鍵は、ｉｄ暗号アルゴリズムに独自のハッシュ関数を、ホームアドレスと、予め定められた満了時間（たとえば、１時間）との関連に適用することによって求められる。ＩＰＫＧは、ｉｄ暗号アルゴリズムを使用して秘密鍵を作り、ＩＰセキュリティ・アソシエーションを使用して暗号化された移動ノード１３５に、作成した秘密鍵と満了時間を返信する（ブロック２１０）。この作成された公開鍵と秘密鍵は、認証あるいは暗号化に使用される。個別暗号化アルゴリズムでは、秘密鍵を生成する際に、ＩＰＫＧのみに知られた秘密が使用される。ゆえに、ディフィ・ヘルマンが提唱するアルゴリズムとは異なり、暗号アルゴリズムの公開パラメータは使用されないので、移動ノード１３５、ホームエージェント１４５、および通信先ノード１４２には公開パラメータが予めプログラミングされていない。秘密マスターキーの有効時間が満了しあるいは失効時間が迫ってきた場合、公開パラメータが更新される。

【００２３】個別暗号化方式は、暗号化アルゴリズムと解読アルゴリズムを含む。暗号化された対象（すなわち、暗号文）は、以下のアルゴリズムを利用して求められる。

ｃｉｐｈｅｒｔｅｘｔ＝ＥＮＣＲＹＰＴ（ｃｏｎｔｅｎｔｓ、ＩＰｕＫ、Ｐａｒａｍｓ）

上記アルゴリズムにおいて、

ｃｉｐｈｅｒｔｅｘｔ・・・暗号文

ＥＮＣＲＹＰＴ・・・メッセージ本文を暗号化するための個別暗号化アルゴリズム

ｃｏｎｔｅｎｔｓ・・・保護するメッセージ本文

ＩＰｕＫ・・・移動ノードが用いる個別公開鍵

Ｐａｒａｍｓ・・・ＩＰＫＧの公開暗号パラメータ

をそれぞれ意味する。なお、ＩＰｕＫ＝Ｈ（ＩＤ、ｔｉｍｅ）が成立する場合では、

Ｈ・・・ＩＤから公開鍵を作るために使用される、個別アルゴリズムにユニークなハッシング・アルゴリズム

ＩＤ・・・鍵を作るために使用される公開識別子
ｔｉｍｅ・・・ＳＮＴＰ（ＳｉｍｐｌｅＮｅｔｗｏｒｋ　Ｔｉｍｅ　Ｐｒｏｔｏｃｏｌ）バージョン４によって示される、公開鍵／秘密鍵のＩＰｖ６満了時間をそれぞれ意味する。暗号文は、以下のアルゴリズムを使用して解読される。
ｃｏｎｔｅｎｔｓ＝ＤＥＣＲＹＰＴ（ｃｉｐｈｅｒｔｅｘｔ,ＩＰｒＫ,Ｐａｒａｍｓ）
上記アルゴリズムにおいて、
ＩＰｒＫ・・・移動ノードの秘密鍵
ＤＥＣＲＹＰＴ・・・暗号文を解読する際に用いる個別解読アルゴリズム
をそれぞれ意味する。
メッセージ認証コード（ｍｅｓｓａｇｅ　ａｕｔｈｅｎｔｃａｔｉｏｎ　ｃｏｄｅ：ＭＡＣ）は、以下の理論から算出される。
ｍａｃ＝ＭＡＣ（ｃｏｎｔｅｎｔｓ,ｓｙｍＫ）
上記アルゴリズムにおいて、
ｍａｃ・・・演算された認証トークン
ＭＡＣ・・・メッセージの認証トークンを演算するために使用される、対称キー別メッセージ認証コードアルゴリズム
ｃｏｎｔｅｎｔｓ・・・認証されるメッセージ本文
ｓｙｍＫ・・・ｍａｃの送信者と受信者によって共有される対称キー

【００２４】移動ノード１３５とホームエージェント１４５間には、ＩＰセキュリティ・アソシエーションの確立が求められる。ＩＰセキュリティ・アソシエーションは、暗号パラメータ情報と秘密鍵情報を安全に移動ノード１３５に伝送するための取り決めである。移動ノード１３５、ホームエージェント１４５、および通信先ノード１４２はそれぞれ個別暗号化システムを実行する。ホームエージェント１４５は、個別秘密鍵生成部（ＩＰＫＧ）としての機能を提供し、あるいはＩＰＫＧへ安全にアクセスするための手段である。移動ノード１３５は、はじめに公開暗号パラメータとともに、移動ノード自身の１２８ビットのＩＰｖ６ホームアドレス（ＨｏＡ）に関連した、個別公開鍵と秘密鍵のペアを有するよう構成されている。

【００２５】次に移動ノード１３５は、通信先ノード１４２との交信開始に際して、通信先ノード１４２にパラメータ検索開始メッセージを送信する（ブロック２２０）。ここで、通信先ノード１４２がその移動ノードに関連する公開暗号パラメータを記録済みあるいはキャッシュ済みでない場合、通信先ノード１４２は、移動ノード１３５が属するホームエージェント１４５からパラメータをダウンロードする（ブロック２３０およびブロック２４０）。次に通信先ノード１４２は、移動ノードの公開鍵によって暗号化された、共有鍵を移動ノード１３５に送出する（ブロック２５０）。

【００２６】そして、移動ノード１３５は安全に対応情報更新を送信することができる（ステップ２６０）。移動ノード１３５は、共有鍵によって保護した対応情報更新を通信先ノード１４２に送る。通信先ノード１４２は、共有鍵によって対応情報更新を認証する。さらに通信先ノード１４２は、共有鍵を使って認証トークンを認証する。したがって、認証のために、移動ノードが公開鍵あるいはその他証明書を送信する必要はない。また、対称キー方式が採用されているので、対応情報更新を認証するために、潜在的に時間がかかる公開化鍵暗号化処理を対応情報更新ごとに行う必要もない。通信先ノード１４２は、対応情報受け取り通知（Ｂｉｎｄｉｎｇ　Ａｃｋｎｏｗｌｅｄｇｅｍｅｎｔ：ＢＡ）を移動ノード１３５に送信する(ステップ２７０)。

【００２７】秘密鍵と暗号パラメータを安全に移動ノード１３５に配布するためのプロトコルは、以下の２つのメッセージを含む。
１）　ＡＢＫ　Ｒｅｑｕｅｓｔ：秘密鍵とパラメータを要求
２）　ＡＢＫ　Ｒｅｐｌｙ：秘密鍵とパラメータを返信

【００２８】ホームエージェントから暗号パラメータを取得し、アドレス・ベースド・キーを用いた共有鍵を確立するためのプロトコルは、以下に示す４つのメッセージを含む。
１）　ＡＢＫｐ１：移動ノード(ＭＮ)が通信先ノード(ＣＮ)にパラメータをキャッシュする指示
２）　ＡＢＫｐ２：通信先ノード(ＣＮ)がホームエージェント(ＨＡ)にパラメータを要求
３）　ＡＢＫｐ３：ホームエージェント(ＨＡ)が通信先ノード(ＣＮ)にパラメータを返信
４）　ＡＢＫｐ４：通信先ノード(ＣＮ)は、移動ノード(ＭＮ)から受け取ったパラメータ・キャッシュ指示に応答
通信先ノード１４２がホームエージェント１４５が持つパラメータを既にキャッシュしている場合、ＡＢＫｐ２メッセージとＡＢＫｐ３メッセージは不要である。さらに、以下の標準モバイルＩＰｖ６対応情報更新（ＢＵ）が使用される。
１）　ＢＵ：移動ノード（ＭＮ）は通信先ノード（ＣＮ）へ対応情報更新＋対応情報認証データを渡す。
２）　ＢＡ：通信先ノード（ＣＮ）は移動ノード（ＭＮ）に対応情報受け取り通知を行う。これらメッセージについての詳細は以下に示す通りである。

【００２９】ホームエージェント１４５は、そのドメインに含まれるすべての移動ノードのためのＩＰＫＧとして機能しうる。ホームエージェント１４５は、公開暗号パラメータ（Ｐａｒａｍｓ）を生成する。このパラメータは、個別暗号化アルゴリズムに使用される。移動ノード１３５は、ホームエージェント１４５によって、１２８ビットのインターネット・プロトコル・バージョン６

（ＩＰｖ６）ホームアドレス（ＨｏＡ）を割り当てられる。このホームアドレスは、基幹モバイルＩＰｖ６規格に準拠した、ホームエージェント１４５と移動ノード１３５間のＩＰセキュリティ・アソシエーションを構成する基礎的枠組みである。

【００３０】移動ノード１３５は、ホームエージェントに秘密鍵ＩＰｒＫと公開暗号パラメータを要求する。移動ノードによるこの要求は、対応情報更新の伝送に先立って、いつ実行されても良い。上述したように、対応情報更新の伝送とは、予め確立されたＩＰセキュリティ・アソシエーションを利用した、ホームエージェント１４５と移動ノード１３５間でのメッセージのやり取りのことである。ホームエージェント１４５は、秘密鍵（ＩＰｒＫ）、公開パラメータ、パラメータのバージョン番号、および公開鍵／秘密鍵の期限が満了する時間を示すＳＮＴＰを移動ノードに返信する。移動ノード１３５は、自身の公開鍵をＩＰｕＫ＝Ｈ（ホームアドレス、満了時間）で定義される公式から算出することができる。移動ノード１３５が有するアドレス・ベースド・キーによって自身を構成および更新するためのメッセージ・フォーマットは以下に示される。

【００３１】移動ノード１３５は、通信先ノード１４２が公開暗号パラメータの要求を開始するように、ＡＢＫｐ１メッセージを通信先ノードに伝達する。パケット送信元アドレスは、移動ノード１３５のホームアドレス（ＨｏＡ）である。ＡＢＫｐ１メッセージは、パラメータのバージョン番号であるパラメータ・バージョン（Ｐａｒａｍｓ　ｖｅｒ）と、公開鍵／秘密鍵ペアが失効する時間である、時間ＳＮＴＰ領域を含む。

【００３２】ＡＢＫｐ１メッセージを受け取ると、通信先ノード１４２は、移動ノード１３５のホームアドレス（ＨｏＡ）が有するサブネット・プレフィックスとして、モバイルＩＰｖ６ホームエージェント・エニキャスト・アドレス（ＨＡＡ）を定める。通信先ノード１４２は、ＨＡＡを定めるためにキャッシュされた、正しいパラメータ番号が付けられたパラメータと、それに対応する失効時間が存在するかを確認する。パラメータとその失効時間の存在が確認されたなら、通信先ノード１４２はホームエージェントとの間でＡＢＫｐ２メッセージとＡＢＫｐ３メッセージを送信する必要はなく、ＡＢＫｐ４メッセージを移動ノードに送ってもよい。

【００３３】一方、通信先ノード１４２が正しいバージョン番号付けがされていないパラメータ、あるいは経過した失効時間をキャッシュしている場合がある。この場合、通信先ノード１４２は、宛先アドレスＨＡＡなどを利用して、ＡＢＫｐ２メッセージをホームエージェント１４５に送る。なお、特定のホームエージェント（ＨＡ）１４５に関連する公開鍵／秘密鍵のペアに関して、その失効時間は共通であるものとする。

【００３４】通信先ノード１４２がＡＢＫｐ２メッセージとＡＢＫｐ３メッセージを送る必要がある場合、ＡＢＫｐ２メッセージは以下に示す領域を含む。

ＨｏＡ…移動ノードのホームアドレス

Ｎｍａｃ…ホームエージェントに依存した、暫定メッセージ認証コード

暫定メッセージ認証コードは、以下に示すアルゴリズムで定義される。

ｎｍａｃ＝ＭＡＣ（ＳＨＡ１（ＨＡＡ,Ｎ１）,ｋ_ＣＮ）

上記アルゴリズムにおいて、

Ｎ１：暫定

ｋ_ＣＮ：通信先ノードにユニークな秘密鍵

【００３５】暫定コードＮ１は好ましくは定期的に復元されるが、通信先ノード１４２と同じ時間帯に動作するあらゆるホームエージェント１４５には、同一の暫定コードが用いられる。通信先ノード１４２は、最近使用した暫定コードをキャッシュしてもよい。

【００３６】ＡＢＫｐ２メッセージを受け取ると、ホームエージェント１４５は移動ノード１３５のホームアドレス（ＨｏＡ）が既に把握されているかを決定する。そしてホームエージェント１４５は、以下のメッセージ領域を含めて、ＡＢＫｐ３メッセージを通信先ノード１４２に送る。

Ｐａｒａｍｓ．

Ｐａｒａｍｓ_ｖｅｒ：パラメータのバージョン番号

ｔｉｍｅ：公開鍵／秘密鍵ペアのＳＮＴＰ失効時間

ＡＦ：アドレス変換許可フラグ

ｎｍａｃ

【００３７】移動ノードのホームアドレス（ＨｏＡ）が、把握されていないホームアドレスである場合、パラメータ値はホームエージェント（ＨＡ）１４５によってゼロに設定される。アドレス変換認証フラグが設定されていない場合、移動ノード１３５は普遍的なインターフェース識別子を使用してもよい。通信先ノード１４２は、ホームアドレスのインターフェース識別子と気付アドレスのインターフェース識別子が同じであるか決定する。アドレス変換認証フラグが設定されている場合、気付アドレスによるルーティング変更を許可するための、上記インターフェース識別子とは異なる媒体が使用されてもよい。ＡＢＫｐ３メッセージを受け取ると、通信先ノード１４２はパラメータ値を確認し、ＭＡＣ（ＳＨＡ１（ＨＡＡ,Ｎ１）,ｋ_ＣＮ）式を計算する。パラメータ値がゼロに設定されている場合、または暫定的メッセージ認証コードと計算されたメッセージ認証コード（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）値が合致しない場合、気付アドレスは認証されない。なお、通信先ノード１４２はエラーメッセージを送らない。パラメータ値がゼロに設定されていない場合、通信先ノード１４２はホームエージェント・エニキャスト・アドレス（ＡＢＰｋ３メッセージの送信元アドレ

ス）、パラメータ、パラメータのバージョン番号、カレント・キー失効時間、およびアドレス変換認証許可フラグをキャッシュする。ＡＢＫｐ４メッセージは、以下に示す領域を有する。

Ｅ＝ＥＮＣＲＹＰＴ（ｋ_ｍ，ＩＰｕＫ，Ｐａｒａｍｓ）

上記アルゴリズムでは、

ｋ_ｍ＝ＳＨＡ１（ＨｏＡ，ｋ_ＣＮ）。

【００３８】ｋ_ｍは、通信先ノード１４２が作成し、移動ノード１３５と共有する鍵を表わす。共有鍵は、移動ノード１３５のホームアドレス（ＨｏＡ）と公開鍵／秘密鍵の失効時間から算出される、移動ノード１３５の公開鍵によって暗号化されている。ＡＢＫｐ４メッセージを受け取ると、移動ノード１３５はｋ_ｍ＝ＤＥＣＲＹＰＴ（Ｅ，ＩＰｒＫ，Ｐａｒａｍｓ）を使用して対応情報更新を求める。

【００３９】対応情報更新メッセージは、基幹モバイルＩＰｖ６処理にしたがって、移動ノード１３５から通信先ノード１４２に送られる。標準領域に加えて、対応情報更新メッセージは対応情報許可データオプション領域を含む。対応情報許可データオプション領域は、以下に示す領域で算出されたメッセージ認証コード（ＭＡＣ）を含む。

（ホームアドレスを含む）対応情報更新の内容

ｋ_ｒ…移動ノードによって生成された不規則値

認証符号は、以下に示す数式から計算される。

ｍａｃ＝ＭＡＣ（ＳＨＡ１（ＢＵ，ｋ_ｒ），ｋ）

ここで、セッション鍵はｋ＝ＳＨＡ１（ｋ_ｍ｜ｋ_ｒ）で算出される。

【００４０】対応情報更新受信の際に、移動ノード１３５のホームアドレス（ＨｏＡ）にアドレス変換許可フラグＡＦが設定されていない場合、通信先ノード１４２は、提示された気付アドレス（ＣｏＡ）のインターフェース識別子がホームアドレス（ＨｏＡ）のインターフェース識別子に一致するかを判断する。なお、ホームアドレスは対応情報更新パケットのホームアドレス・オプション領域に含まれる。インターフェース識別子が一致しない場合、通信先ノード１４２は適切なエラーコードを表示したバインディング受け取り通知を送信する。

【００４１】アドレス変換認証フラグＡＦが設定されている場合、通信先ノードはアドレス変換許可アルゴリズムを実行して、移動ノード１３５がアドレス変換をして良いかを決定する。

【００４２】アドレス変換認証フラグＡＦが設定されておらず、提示された気付アドレス（ＣｏＡ）のインターフェース識別子が対応情報更新パケットのホームアドレスオプション内のホームアドレス（ＨｏＡ）のインターフェース識別子に一致する場合がある。また、アドレス変換認証フラグＡＦが設定されており、移動ノードでのアドレス変換が認証されている場合がある。いずれの場合であっても、通信先ノード１４２は、ｋ_ｍ＝ＳＨＡ１（ＨｏＡ，ｋ_ＣＮ）を計算した後、ｋ＝ＳＨＡ１（ｋ_ｍ｜ｋ_ｒ）を算出する。そして、対応情報認証データオプションの認証符号から得られるｍａｃ値を、ＭＡＣ（ＳＨＡ１（ＢＵ，ｋ_ｒ），ｋ）を計算して得られる値と比較することにより、通信先ノード１４２は対応情報更新を認証する。それぞれの値が一致した場合、通信先ノード１４２は、認証が受け付けられたことを示す対応情報受け取り通知（ＢＡ）メッセージを送る。もしくは、通信先ノード１４２は、認証が失敗したことを示す対応情報受け取り通知（ＢＡ）メッセージを送る。

【００４３】ホームエージェント（ＨＡ）１４５がアドレス変換許可フラグを設定する指示をＡＢＰｋ３メッセージにて示さない限り、移動ノード１３５は、ホームアドレスのインターフェース識別子と同じインターフェース識別子を気付アドレスに使用する。アドレス交換認証フラグが設定されていないにもかかわらず、インターフェース識別子が異なっていると対応情報更新が示す場合がある。この場合、通信先ノード１４２は対応情報更新の受け取りを拒否して、対応情報受け取りエラーを移動ノード１３５に送る。

【００４４】ホームエージェント１４５がアドレス変換認証フラグを設定して、何らかの処理が行われていることを示している場合、移動ノード１３５のホームアドレスのインターフェース識別子は気付アドレスのそれと異なっても良い。ホームアドレスと気付アドレスそれぞれのインターフェース識別子が異なることによって、特定ホームアドレス（ＨｏＡ）を持つ移動ノード１３５が特定気付アドレス（ＣｏＡ）へ変更することを認める許可方法を、通信先ノード１４２と移動ノード１３５は共有する。ホームアドレスを気付アドレスへ変更する例として、暗号化されたアドレスやＡＡＡなどがある。

【００４５】移動ノードとそのホームアドレスの対応関係は認証される。通信先ノード１４２は、ホームエージェント（ＨＡ）１４５からパラメータを直接受け取る。さらに、共有鍵を解読できるのはその資格がある移動ノード１３５に限られる。共有鍵は、対応情報更新を認証する、セッション鍵を作るために使用される。

【００４６】移動ノード１３５が、数多くのＡＢＫｐ１メッセージを送って通信先ノード１４２を満たす場合、通信先ノード１４２はメッセージを受け取るごとにパラメータ・テーブルを確認する。そして、通信先ノード１４２が関連するホームエージェント１４５のパラメータを持っているかを判断する。メッセージに関連する、ホームエージェントのパラメータがない場合、通信先ノード１４２はホームエージェント１４５にＡＢＫｐ２メッセージを送って、そのパラメータを要求する。パラメータが失効しない限り、通信先ノード１４２は、ＡＢＫｐ２メッセージを同一のホームエージェント１４５に再送しない。通信先ノード１４２は、メッセージのやり取りを主導しない。ホームエージェント１４５が数多くのＡ

ＢＫｐ２メッセージで占められた場合、ホームエージェント１４５はそのドメイン外のホームアドレス（ＨｏＡ）を含むすべてのメッセージを破棄する。

【００４７】暫定メッセージ認証コード（ｎｍａｃ）を使用することによって、通信先ノード１４２との通信を試みる、もしくは多数のＡＢＫｐ３メッセージを送信して通信先ノード１４２を占有しようとする、悪意の第３者を防ぐことができる。多数のＡＢＫｐ４メッセージに関して、移動ノード１３５がＡＢＫｐ１メッセージの形成に関与しなかった場合、移動ノード１３５はそれらのあらゆるメッセージを無視する。通信先ノードは、メッセージ認証コードが認証されない対応情報更新メッセージを無視する。移動ノード１３５は、対応情報更新を送信した先ではないノードから返答された対応情報の受け取り通知（ＢＡ）メッセージを無視する。

【００４８】移動ノード１３５、通信先ノード１４２、およびホームエージェント１４５のいずれかのうちの２つの間を通るパスで、送られたメッセージを悪意の第三者が変更できるとすれば、最悪の場合は対応情報更新それ自体の伝送が失敗する。通信先ノード１４２は、移動ノード・パケットを、更新される前の気付アドレス（ＣｏＡ）に引き続き送る。ＡＢＫｐ１からＡＢＫｐ３の各メッセージは署名されていないので、それらが変更される可能性は残る。しかし、ＡＢＫｐ４メッセージが認証されると同様、暗号化されたなら、ＡＢＫｐ４メッセージは第三者から変更されない。対応情報更新はメッセージ認証コードによって保護されているので、悪意を持った第三者からデータ変更されない。

【００４９】他の実施形態で、通信先ノード１４２がホームエージェント１４５用の標準公開鍵証明書を含んでいる場合、通信先ノード１４２は、ＡＢＫｐ２からＡＢＫｐ３間をトランザクトする、ＴＬＳ（Ｔｒａｎｓｐｏｒｔ　Ｌｅｖｅｌ　Ｓｅｃｕｒｉｔｙ,ＲＦＣ２２４６）プロトコル等を利用する。このＴＬＳプロトコルによって、ホームエージェント・トランザクションへの妨害を防げる。

【００５０】移動ノード１３５はリダイレクト攻撃を起こしうる。この場合、リダイレクト攻撃の被害者を収容する異なるサブネットの虚偽気付アドレス（ＣｏＡ）を含んだ、対応情報更新が通信先ノード１４２に送られる。通信先ノード１４２は、リダイレクト攻撃の被害者が移動ノードのトラヒックにまったく興味を持っていなくても、移動ノードのトラヒックを被害者にリダイレクトする。気付アドレス（ＣｏＡ）も形成するよう、ホームエージェント１４５から移動ノード１３５に割り当てられたインターフェース識別子を、移動ノード１３５のホームアドレス（ＨｏＡ）に使用するように移動ノード１３５に要求することによって、リダイレクト攻撃を防止できる。さらに、インターフェース識別子をホームアドレスに使用することで、移動ノード１３５は、自身に対応する気付アドレス（ＣｏＡ）以外のアドレスを異なるノードが形成することを防ぐことができる。移動ノード１３５は、すべての気付けアドレス（ＣｏＡ）に、同じインターフェース識別子を使用する。同じ識別子を使用してもルート最適化は制限されない。なぜなら、ルート最適化されたパケットは、いずれにせよ、ホームアドレスを含むホームアドレス・オプションを含むからである。

【００５１】鍵が失効したりパラメータが変更した場合、アドレス・ベースド・キー（ＡＢＫ）分配プロトコルは、最初に、ホームエージェント１４５からアドレス・ベースド・キー（ＡＢＫ）を（場合によっては定期的に）移動ノード１３５に提供する。ＡＢＫ分配プロトコルは、たとえばＩＡＮＡ（Ｉｎｔｅｒｎｅｔ　Ａｓｓｉｇｎｅｄ　Ｎｕｍｂｅｒ　Ａｕｔｈｏｒｉｔｙ）によって割り当てられるべきポートに、ＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）トランスポートを利用する。ＡＢＫプロトコルは、ＩＰｓｅｃＥＳＰ（ｅｎｃａｐｓｕｌａｔｉｎｇ　ｓｅｃｕｒｉｔｙ　ｐａｙｌｏａｄ）と、標準モバイルＩＰｖ６規格によって定義された、ホームエージェント／移動ノードセキュリティ・アソシエーションを用いて保護される。ＡＢＫプロトコルは、ＡＢＫ要求とＡＢＫ応答の２つのメッセージを含むプロトコルである。

【００５２】図３は、ＡＢＫ要求メッセージの構成を示すものである。ＡＢＫ要求メッセージが、新しいＡＢＫを要求するために、移動ノード１３５からホームエージェント１４５に送られる。このメッセージのソースアドレスは、移動ノードのホームアドレスである。宛先アドレスは、ホームエージェント・アドレスである。ＡＢＫメッセージには、ホームエージェントと移動ノード間で設立されるセキュリティ・アソシエーションを表わすための、ＥＳＰ―ＩＰｓｅｃヘッダ等のＩＰｓｅｃヘッダが含まれても良い。また、メッセージを含むパケットは共有鍵を使って暗号化されてもよい。ＡＢＫ要求メッセージに含まれる識別子のメッセージ類型コード領域３００には例えば５などの数値が設定される。アルゴリズム識別子番号領域３１０は、ゼロ以外の、連続した４バイトのアルゴリズム識別子レコードの番号である。アルゴリズム識別子領域３２０は、ＩＡＮＡによって各レコードに割り当てられた、２バイト個別暗号化アルゴリズム識別子を有する。パラメータ・バージョン番号領域３３０は、アルゴリズム識別子を示す、２バイトのパラメータ・バージョン番号を含む。

【００５３】移動ノード１３５はホームネットワークに在圏しない場合、メッセージ送信に先立って、気付アドレス（ＣｏＡ）とホームアドレス（ＨｏＡ）を有効に結びつける。そして移動ノード１３５は、ホームエージェント１４５へメッセージを逆トンネルすることで、他のサブネットへの進入フィルタリングを回避する。移動ノ

ード１３５は、それが対応するアルゴリズムを示した、識別子に基づく暗号化アルゴリズム識別子リストと、移動ノード１３５に知られているパラメータの最新バージョン番号を持っている。個別暗号化アルゴリズム識別子リストは、移動ノードにとって好ましい順番、たとえばもっとも好ましいアルゴリズムから優先して並べても良い。

【００５４】ＩＰｓｅｃセキュリティ・アソシエーションは、有効なホームアドレス（ＨｏＡｓ）を割り当てられた移動ノード１３５のみ、ホームエージェント１４５と通信できることを保証する。ＡＢＫ要求を受領すると、パラメータ・バージョン番号が最新のバージョン番号に合致していない、アルゴリズム識別子リストに含まれる各アルゴリズムのために、ホームエージェント１４５は秘密鍵（ＩＰｒＫ）を算出する。最初に、ホームエージェント１４５は、パケットの送信元アドレス（公開識別子としてのホームアドレス等を指す）と、ＳＮＴＰ失効時間を基に公開鍵を作る。次にホームエージェント１４５は、公開鍵と、パラメータと、アルゴリズムから秘密鍵を作る。秘密鍵の生成結果は、ＡＢＫ応答メッセージで移動ノード１３４に応答される。

【００５５】図４は、ＡＢＫ応答メッセージの構成を示すものである。ＡＢＫ応答メッセージは、移動ノード１３５から要求されホームエージェント１４５に対応する、アルゴリズムに対応するパラメータのリストを含む。さらに、移動ノード１３５が公開鍵を算出した際に使用した、（鍵の）失効時間値がＡＢＫ応答メッセージに含まれる。ＩＰ領域に関して、ＡＢＫ応答メッセージのソースアドレスは、ホームエージェント・アドレスが相当する。宛先アドレスは、移動ノードのホームアドレス（ＨｏＡ）が相当する。ＩＰヘッダに関し、ホームエージェント／移動ノードのセキュリティ・アソシエーションにはＥＳＰ－ＩＰｓｅｃヘッダが付与され、パケット本体は共有鍵で暗号化される。

【００５６】メッセージ領域の構成に関し、ＡＢＫメッセージ類型コード領域４００には例えば６などの数値が設定される。このコードによって、ＡＢＫ応答メッセージは他のメッセージと区分けされる。キー失効時間領域４１０は、鍵が失効する時間を示す、４バイトの正数を含む。パラメータ／キー番号レコード領域４２０は、アルゴリズムごとの可変長レコード（従うべきパラメータ・レコードとキー・レコード）の番号を含む。それぞれのパラメータ・レコードとキー・レコードに関し、パラメータ／キー・レコード長領域４３０は、アルゴリズム識別子領域４４０と、パラメータ・バージョン番号領域４５０と、パラメータ＋秘密鍵リスト領域４６０を含む、従うべきパラメータ・レコードの長さ（バイト）を示す。アルゴリズム識別子領域４４０は、各レコードに対してＩＡＮＡによって割り当てられた、２バイトの個別暗号化アルゴリズム識別子を含む。パラメータ・バージョン番号領域４５０は、アルゴリズム識別子を示す、２バイトのパラメータ・バージョン番号を含む。パラメータ＋秘密鍵リスト領域４６０は、アルゴリズム識別子規格によってそのフォーマットが指定された、可変長パラメータと秘密鍵リストを含む。

【００５７】ＡＢＫ要求に応じて、ホームエージェント１４５は、暗号化を施し、かつ、適切なＥＳＰ保護ヘッダを付けて、ＡＢＫ応答メッセージを返送する。移動ノード１３５がホームネットワークに属していない場合、ＡＢＫ応答メッセージは気付アドレス（ＣｏＡ）を通じて移動ノード１３５に渡される。この仕組みは、トラフィックが移動ノード１３５のホームアドレス（ＨｏＡ）を通じてルーティングされる流れと同じである。移動ノード１３５によって要求されたいかなるアルゴリズムにホームエージェント１４５が対応しない場合、キー失効時間領域４１０とパラメータ／キー・レコード番号領域４２０はそれぞれゼロを示す。一方、移動ノードが要求するアルゴリズムをホームエージェントがサポートしている場合、各々の領域はゼロ以外の値を示す。ホームエージェント１４５が特定のアルゴリズムに対応しない場合、指示されたアルゴリズムのアルゴリズム識別子領域４４０に、レコードが格納される。また、アルゴリズムが対応しない場合は、パラメータ・バージョン番号領域４５０はゼロを示し、パラメータ＋秘密鍵領域４６０は使用されない。

【００５８】移動ノード１３５に対応する特定のアルゴリズムに対する、ＡＢＫ要求のパラメータ・バージョンが現在動作しているバージョンである場合、レコードは要求されたアルゴリズムのアルゴリズム識別子領域４４０と現行のパラメータバージョン番号領域４５０に格納される。しかし、パラメータ＋秘密鍵領域４６０は使用されない。移動ノード１３５は、キャッシュしたパラメータと秘密鍵を、パラメータが変更、あるいは鍵が失効するまで使用し続ける。ＩＰｓｅｃセキュリティ・アソシエーションとは、ホームエージェント１４５が移動ノード１３５にＡＢＫ応答メッセージを送信できるよう保証するコネクションである。ＡＢＫ応答メッセージを受けると、移動ノードは対応情報更新を保護するために、アルゴリズムごとに秘密鍵とパラメータをキャッシュする。使用している秘密鍵が失効すると、新しい秘密鍵を発行するために、移動ノード１３５は対応する個別暗号化アルゴリズムをホームエージェントに要求する。

【００５９】パラメータ初期化過程では、移動ノード１３５は、ホームエージェント１４５から受け取ったパラメータを初期化するように通信先ノード１４２に要求する。移動ノード１３５は、自身が有する秘密鍵もしくはパラメータを変更する際、パラメータ初期化プロトコルを実行する。パラメータ初期化プロトコルは、ＡＢＫ分配プロトコルとして使われる、ＩＡＮＡ送り先オプションヘッダに割り当てられたポートで、ＴＣＰプロトコル

を使う。移動ノード１３５は、自身がプロトコルを開始する際にホームネットワークにいない場合、ホームエージェント１４５を経由して、ＡＢＫｐ１メッセージを通信先ノード１４２に逆トンネルして、プロトコルを開始する。ＡＢＫｐ４メッセージは、標準モバイルＩＰ機構によって、ホームエージェント１４５を経由して移動ノード１３５に返答される。ＡＢＫｐ２メッセージとＡＢＫｐ３メッセージは、通信先ノード１４２とホームエージェント１４５の間でやり取りされる。

【００６０】図５はＡＢＫｐ１メッセージの構成を示す。移動ノード１３５がホームネットワークに在圏しない場合、ＡＢＫｐ１メッセージは移動ノード１３５からホームエージェント１４５を経由して、対応情報更新を保護するためのプロトコルとして通信先ノード１４２に逆トンネルされる。この際の発信元アドレスは、移動ノード１３５のホームアドレスである。宛先アドレスは、通信先ノード１４２のアドレスである。他のメッセージと区別するため、メッセージ類型コード５００には例えば１などの数値が設定される。アルゴリズム識別子番号領域５１０は、ゼロよりも大きいの、連続した４バイトのアルゴリズム識別子レコード番号５２０を含む。アルゴリズム識別子領域５２０は、ＩＡＮＡによって各レコードに割り当てられた、２バイトの識別子に基づく暗号化アルゴリズム識別子を含む。パラメータ・バージョン番号領域５３０は、アルゴリズム識別子に付与される、２バイトのパラメータ・バージョン番号である。パラメータ・バージョン番号とは、移動ノード１３５によって現在保持されているパラメータ・バージョンを特定する番号のことである。キー失効時間領域５４０は、移動ノードが持つキーの失効時間を特定する、４バイトのＳＮＴＰ時間である。

【００６１】図６は、ＡＢＫｐ２メッセージの構成を示す。ＡＢＫｐ２メッセージは、通信先ノード１４２によってホームエージェント１４５に送信される。ＡＢＫｐ２メッセージの発信元アドレスは、通信先ノード１４２のアドレスである。宛先アドレスは、移動ノードのサブネット内に位置するホームエージェント・エニィキャスト・アドレスである。このホームエージェント・エニィキャスト・アドレスは、移動ノード１３５が含む、ホームアドレス・サブネット・プレフィックスによって決定される。メッセージ領域は、メッセージ類型領域６００を含む。そして、メッセージごとにメッセージ類型コードが例えば２などの異なる数字で示される。メッセージの送受信を無視する場合、予備領域６１０はゼロに設定される。暫定メッセージ認証コード領域６２０では、暫定のメッセージ認証コード（１６０ビットＨ－ＭＡＣ　ＳＨＡ－１）を特定する。ホームアドレス領域６３０では、移動ノード１３５のホームアドレスを特定する。アルゴリズム識別子番号領域６４０は、ゼロ以外の、連続した２バイト・アルゴリズム識別子レコードの番号を特定する。アルゴリズム識別子リスト領域６５０は、ＩＡＮＡまたは他のエンティティによって各レコードに割り当てられた、２バイト個別暗号化アルゴリズムを特定する。

【００６２】移動ノード１３５から送信されかつＡＢＫｐ１メッセージに含まれ、通信先ノード１４２に対応するアルゴリズムのうち、そのパラメータ・バージョン番号が、通信先ノード１４２によってキャッシュされたパラメータ・バージョン番号と合致しないアルゴリズムがある。アルゴリズム識別子リストでは、そのようなアルゴリズムを特定する。ＡＢＫｐ１メッセージで移動ノード１３５から送信されたリストが含むアルゴリズムの少なくとも１つと合致する、パラメータ・バージョン番号をその内部にキャッシュしている場合、通信先ノード１４２はＡＢＫｐ２メッセージを送信しない。これは、通信ノード１４２が、移動ノード１３５が有するアルゴリズムと合致するアルゴリズムを使用するからである。

【００６３】図７は、ＡＢＫｐ３メッセージの構成を示す。このメッセージの発信元アドレスは、ホームエージェント１４５のアドレスである。宛先アドレスは、通信先ノード１４２のアドレスである。メッセージ領域は、メッセージ類型領域７００を含む。この領域では、ＡＢＫメッセージに対し、例えば３などの固有のメッセージ類型コードが示される。Ａ領域７１０は、未設定コマンドあるいは設定コマンドを特定する。ここで、ホームエージェント１４５がホームアドレス（ＨｏＡ）が使用するインターフェース識別子と同じインターフェース識別子を気付アドレス（ＣｏＡ）にも使用するように、移動ノード１３５に求める場合、未設定コマンドが使用される。これに対し、異なるアドレス変換認証処理が行われる場合、設定コマンドが使用される。予備領域７２０は、メッセージ送信に際してゼロに設定される。暫定メッセージ認証コード領域７３０では、ＡＢＫｐ２メッセージで送信された暫定値と合致する、暫定のメッセージ認証コード（１６０ビットＨ－ＭＡＣ　ＳＨＡ－１）を特定する。

【００６４】パラメータ・レコード番号領域７４０は、可変長パラメータ・レコード番号を識別する。パラメータ・レコード長領域７５０は、各レコードのために、アルゴリズム識別子領域７６０、パラメータ・バージョン番号領域７７０、およびパラメータ領域７８０を含む、パラメータ・レコードの長さ（バイト）を特定する。アルゴリズム識別子領域７６０は、ＩＡＮＡによって各レコードに割り当てられた、２バイトの個別暗号化アルゴリズム識別子を有する。パラメータ・バージョン番号領域７７０は、アルゴリズム識別子に付けられる、２バイトのパラメータ・バージョン番号を含む。パラメータ領域７８０は、アルゴリズム識別子規格にしたがってそのフォーマットが決定される、可変長パラメータ領域７９０を備える。

【００６５】移動ノード１３５のホームアドレス（ＨｏＡ）を示すレコードを持っていない場合、ホームエージェント１４５はパラメータ・レコード番号領域７４０がゼロに設定された、ＡＢＫｐ３メッセージを通信先ノードに応答する。パラメータ・レコード番号領域７４０はゼロに設定されなくても良い。ホームエージェント１４５が、ＡＢＫｐ３メッセージに含まれて送られたリストのいずれのアルゴリズムをもサポートしない場合、アルゴリズム識別子領域７６０に該アルゴリズムを含むレコードを送信する。このレコードでは、パラメータ・バージョン番号領域７７０はゼロに設定され、また、パラメータ領域７８０にパラメータは存在しない。他の実施形態では、ホームエージェント１４５は、そのパラメータを有するＡＢＫｐ２メッセージに含まれた各アルゴリズムのために、パラメータ・レコードを記憶する。

【００６６】図８は、ＡＢＫｐ４メッセージの構成を示す。このメッセージのＩＰアドレス領域に関し、ソースアドレスは通信先ノードのアドレスが該当する。一方、移動ノードのホームアドレスは宛先アドレスである。メッセージは、メッセージ類型領域８００を含む。この領域では、ＡＢＫメッセージに対し、メッセージ類型コードを示す、例えば４などのメッセージ番号が設定される。状態コード領域８１０は、メッセージ状態を示すコードを含む。コード例は、以下に示す通りである。

０・・・正常状態

１・・・アルゴリズムはサポートされていない。移動ノード１３５と通信先ノード１４２がアルゴリズムを共有しない場合、コード「１」が返信される。

２・・・パラメータは失効している。移動ノードと共有するすべてのアルゴリズムに、ホームエージェント１４５によって応答されたパラメータのバージョン番号が、移動ノード１３５によって提供されたパラメータのバージョン番号よりも新しい場合、コード「２」が返信される。

【００６７】アルゴリズム識別子領域８２０は、セッション鍵を作るために通信先ノード１４２によって使用されるアルゴリズムを示す、２バイトのアルゴリズム識別子を含む。暗号化鍵長さ領域８３０は、暗号化されたセッション鍵（Ｅ）の長さをバイト単位で明らかにする。上述したとおり、ＥはＥＮＣＲＹＰＴ（ｋ_ｍ,ＩＰｕＫ,Ｐａｒａｍｓ）と同じ意味である。暗号化されたセッション鍵（Ｅ）は「Ｅ」領域８４０に含まれる。

【００６８】アルゴリズム識別子仕様は、共有鍵および他のデータ、それぞれのフォーマットを含む。通信先ノード１４２は、移動ノード１３５がＡＢＫｐ１メッセージを通じて送るリストの中からアルゴリズムを選択する。選択されたアルゴリズムのパラメータは、ＡＢＫｐ３メッセージを通じてホームエージェント１４５から返答されることで、あるいは、ＡＢＫｐ２もしくはＡＢＫｐ３メッセージが不要な場合、通信先ノード１４２からキャッシュされることで、利用可能である。通信先ノード１４２は、選択されたアルゴリズムの識別子をアルゴリズム識別子領域８２０内に有する。移動ノードはその好みに応じてリストを並び替えているので、通信先ノード１４２は、ＡＢＫｐ１メッセージを通じて移動ノードによって送られたリスト内で最初の順番に最も近いアルゴリズムを選択する。

【００６９】暗号化セッション鍵領域８４０は、移動ノード１３５の公開鍵（移動ノード１３５のホームアドレス（ＨｏＡ）と、キー失効時間から算出）とアルゴリズム・パラメータを使って暗号化された、セッション鍵を含む。上記領域のフォーマットは、アルゴリズムに応じて定められるものであり、アルゴリズム仕様である。移動ノードのホームアドレス（ＨｏＡ）を認識してないとホームエージェント１４５が知らせる場合、通信先ノード１４２は応答メッセージを送らない。

【００７０】通信先ノード１４２は、移動ノード１３５と合意するアルゴリズムをそのパラメータと共に選択できる場合、状態コード領域８１０はゼロに設定され、メッセージの残余部分が占められる。状態コード領域がゼロに設定されていない場合、通信先ノード１４２は他の領域を含まない。通信先ノード１４２と移動ノード１３５が、少なくとも１つのアルゴリズムとパラメータ・バージョンの組み合わせに合意する場合、通信先ノード１４２は合意したアルゴリズムを選択する。組み合わせの選択肢がまったくない場合を除いては、通信先ノード１４２はノン・ゼロ状態コードを送らない。

【００７１】対応情報更新を保護するためにＡＢＫを使っている移動ノード１３５は、既述の通りに算出された認証トークン_ｍａｃ_とともに、標準モバイルＩＰｖ６の対応情報を認証するデータ拡張子を、認証符号領域に含む。上述したように、通信先ノード１４２は認証符号を認証する。認証符号が認証されない場合、通信先ノード１４２はエラー・コード１３７（無効認証）を対応情報確認応答（Ｂｉｎｄｉｎｇ　Ａｃｋｎｏｗｌｅｄｇｅｍｅｎｔ）に送る。アドレス変換認証チェックが失敗した場合、気付けアドレス（ＣｏＡ）には認証されていないことを示す、エラー・コードが移動ノード１３５に送られる。

【００７２】ＡＢＫ対応情報更新にて使用されるべき個別暗号化化アルゴリズムのために、アルゴリズムを示し、ＩＡＮＡによって割り当てられたアルゴリズム類型コード、ＡＢＫ応答メッセージ内のパラメータ＋ＩＰｒＫ領域を表わすフォーマット、ＡＢＫｐ３メッセージ内のパラメータ領域を表わすフォーマット、およびＡＢＫｐ４メッセージ内の暗号化セッション鍵領域を表わすフォーマットを提供する、仕様がある。この仕様は、インターネット技術タスクフォース標準活動によって制定される。また、ＩＡＮＡによって割り当てられるべきプロトコルのために、ＴＣＰソケット番号が求められる。さ

らに移動ノード１３５が、ある気付けアドレス（ＣｏＡ）への変更を認証されない場合は、モバイルＩＰバインディング確認応答エラー・コードが決定されても良い。

【００７３】以上、様々な実施形態を参照しつつ本発明を記載してきたが、本発明は特許請求の範囲に記載した思想および範囲内で種々の変形が可能である。それゆえ、以下の詳細な記述は本発明の好ましい実施形態を実例で示すことを目的としており、本発明を定義するのではないと解釈されるべきである。本発明を定義するのは、すべての関連要素を含む、上記に記載の請求項のみである。

【００７４】

【発明の効果】以上説明したように、この発明によれば、無線通信システムでの対応更新情報を保護することができる。

＊【図面の簡単な説明】

【図１】　無線モバイルアクセスＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）ネットワークの一実施例である。

【図２】　対応情報更新を保護するための、個別暗号化システムの実施例を示すラダー図である。

【図３】　ＡＢＫ要求メッセージの構成例である。

【図４】　ＡＢＫ応答メッセージの構成例である。

【図５】　ＡＢＫｐ１メッセージの構成例である。

【図６】　ＡＢＫｐ２メッセージの構成例である。

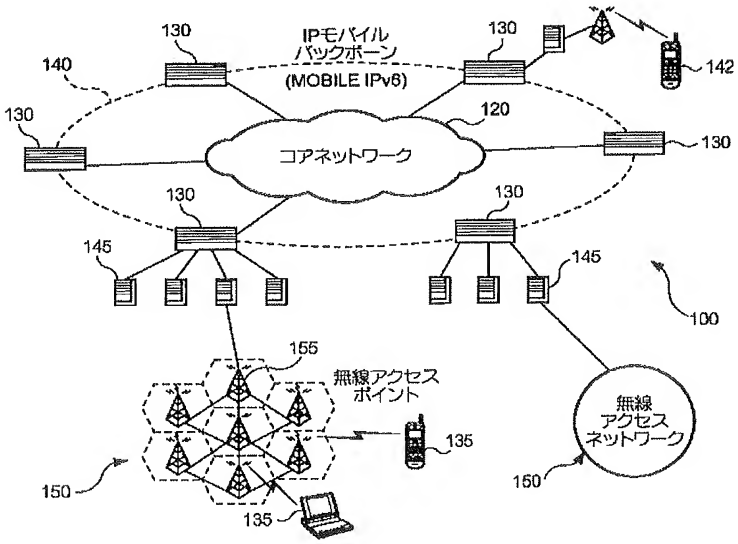
【図７】　ＡＢＫｐ３メッセージの構成例である。

【図８】　ＡＢＫｐ４メッセージの構成例である。

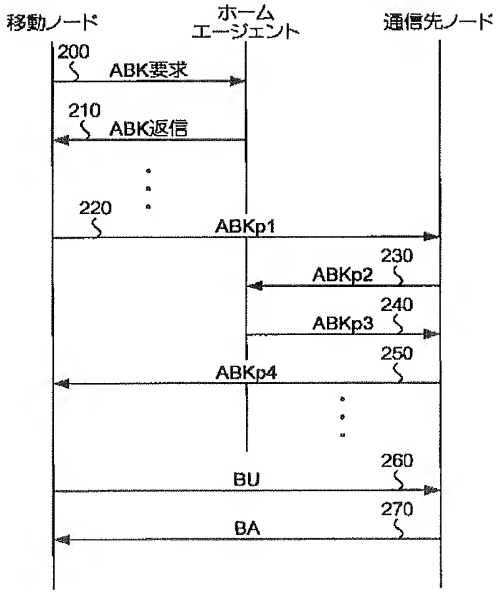
【符号の説明】

１３５・・・移動ノード、１４２・・・通信先ノード、１４５・・・ホームエージェント。

【図１】

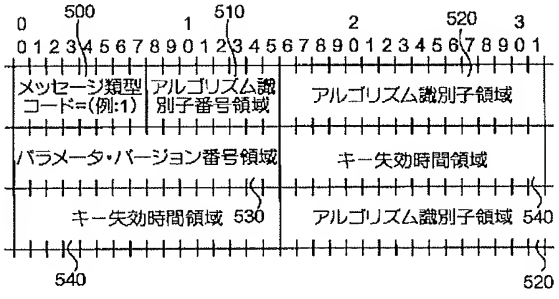


【図２】



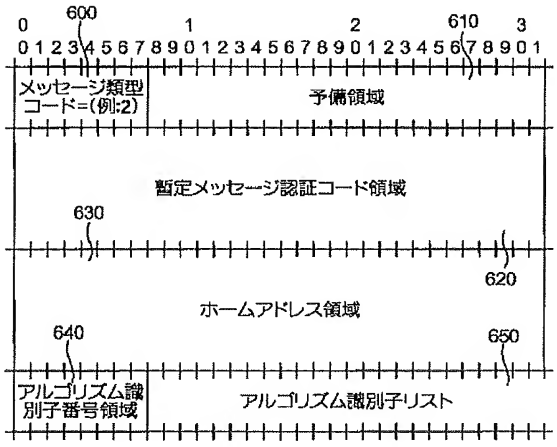
【図３】

【図５】



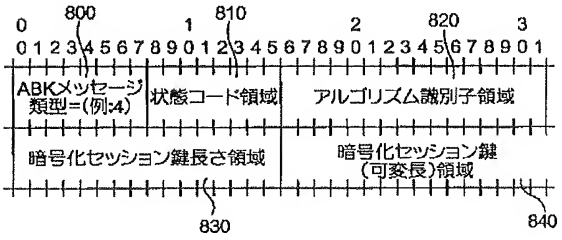
【図４】

【図６】



【図７】

【図８】



フロントページの続き

(72)発明者　ジェームズ　ケンプフ
アメリカ合衆国、カリフォルニア州　94043、マウンテン　ビュー、221　ノース、レングストーフ　４号室
(72)発明者　アナンド　デサイ
アメリカ合衆国、カリフォルニア州　94025、メンロパーク、イーストクリークドライブ　120、12Ａ号室
(72)発明者　オカザキ　サトミ
アメリカ合衆国、カリフォルニア州　94306、パロアルト、シェリダン　アベニュー　410、450号室
(72)発明者　イクィン　リサ　イン
アメリカ合衆国、コネチカット州　06870、オールドグリーンウィッチ、ハブマイヤーレーン　78
(72)発明者　クライグ　ジェントリー
アメリカ合衆国、カリフォルニア州　94041、マウンテンビュー、ムアードライブ　708
(72)発明者　アリス　シルバーバーグ
アメリカ合衆国、カリフォルニア州　95110、サンノゼ、メトロドライブ　181、スイート300

Ｆターム(参考) 5J104 AA16 EA17
5K067 AA30 BB04 BB21 DD17 DD51
EE02 EE10 EE16 HH36

【外国語明細書】

SECURING BINDING UPDATE USING ADDRESS BASED KEYS

RELATED APPLICATIONS

This application claims priority to the earlier filed provisional U.S. patent applications serial number 60/358,177, filed February 19, 2002 and serial number 60/416,029, filed October 3, 2002, both entitled "Securing MIPV6 Binding Update Using Address Based Keys (ABK)," which are incorporated by reference herein.

BACKGROUND

The results of known Mobile IP design work and technical discussions trend toward accepting Return Routability (RR) as the basic technique for securing MIPv6 Binding Update (BU). A wide variety of proposed mechanisms for Return Routability exist. Yet, there is recognition that Return Routability has drawbacks, both in terms of its security properties and also performance.

While identity based cryptosystems are known in the cryptographic community, they have not been used in the networking security community. The Diffie-Hellman technique remains the reigning standard. Moreover, until recently, there have been no known identity based cryptographic algorithms that could be used to perform encryption. The existing algorithms have been restricted to digital signature calculation, and therefore have been limited in scope. Recent work has established new algorithms, based on elliptic curves, which allow encryption to be performed as well.

BRIEF SUMMARY

A system and method are disclosed for securing Binding Update in a wireless telecommunications system. A public key is established using a home address value of the mobile host. Thereafter, a home agent generates a private key using public cryptographic parameters, that corresponds to the mobile host and the public key.

When the mobile host initiates a conversation with a correspondent node, the mobile host sends a message via the home agent to the

correspondent node requesting that the correspondent node obtain the public cryptographic parameters from the home agent. If the correspondent node does not have the cryptographic parameters, the correspondent node obtains the parameters from the home agent. The correspondent node uses the mobile host's home address and the cryptoparameters to encrypt a shared secret key which is sent to the mobile host via the home agent. The mobile host decrypts the shared secret using the private key, and uses the shared secret to calculate a message authentication code on the Binding Update. The correspondent node authenticates the binding update by examining the message authentication code, using the shared secret key.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates an exemplary wireless, mobile access, Internet Protocol network.

FIG. 2 is a ladder diagram illustrating the use of an Identity-based cryptosystem to secure a Binding Update.

FIG. 3 illustrates an exemplary ABK Request message.

FIG. 4 illustrates an exemplary ABK Reply message.

FIG. 5 illustrates an exemplary ABKp1 message.

FIG. 6 illustrates an exemplary ABKp2 message.

FIG. 7 illustrates an exemplary ABKp3 message.

FIG. 8 illustrates an exemplary ABKp4 message.

DETAILED DESCRIPTION

Presently preferred embodiments of a mechanism for securing telecommunication Binding Update are described herein with reference to the drawings, wherein like components are identified with the same references. The security mechanism includes the use of Address Based Keys (ABKs) or other encryption methodsfrom the Weil paring and cryptosystems based on pairing for shared secret encryption. The descriptions contained herein are intended to be exemplary in nature and are not intended to limit the scope of the invention.

A system and method are described for securing MIPv6 Binding Updates using identity-based cryptography. Identity-based cryptography includes a body of cryptographic techniques that allow a client to use a public identifier, such as its IP address, as its public key. The client obtains private keys, along with a set of public cryptoparameters, from an Identity-based Private Key Generator (IPKG). A correspondent wanting to encrypt a message uses the client's public identity along with the public cryptoparameters. The correspondent obtains the public cryptoparameters from the IPKG. The client decrypts the message using its private key.

FIG. 1 illustrates an exemplary wireless, mobile access, Internet Protocol (IP) network 100. The wireless, mobile access, IP network 100 has a fixed node IP data network 120 comprising numerous fixed nodes (not shown), i.e., fixed points of connection or links. Data is communicated within and over the network in accordance with Internet protocols such as Internet protocol version 6, specified as IETF RFC 2460, which is incorporated herein by reference. Built on the core network 120 is a collection of gate routers 130 which collectively form an IP mobile backbone 140 and function, in accordance with the conventional Internet addressing and routing protocols, to route packets of data between source and destination nodes connected to the network. The gate routers 130 forming the IP mobile backbone 140 are themselves nodes of the core network 120 and have unique IP addresses for communication over the core network 120.

Connected to each of the gate routers 130 are servers or routers 145, which also have unique IP addresses and function as Home Agents (HA) to interface mobile hosts, such as Mobile Nodes 135, and Correspondent Nodes 142 to the core network 120. The Mobile Node 135 includes an interface to communicate with the Correspondent node 142, and vice versa. The Correspondent Node 142 may also be mobile. The Mobile Node 135 and Correspondent Node 142 may include different kinds of mobile, wireless communication devices including cellular handsets, cellular telephones, hand-held computers, personal information managers, wireless data terminals, and the like.

The Mobile Node 135 has an established security association with one or more home agents 145 on a home link. The Mobile Node 135 is programmed to detect moves between different points of attachment in the network 100. The Mobile Node 135 can be identified by a Home Address (HoA), i.e., an address of the Mobile Node 135 which does not change as the mobile node moves through the network 100. The Mobile Node 135 acquires a temporary care of address (COA) in each visited location of the network 100. The Mobile Node 135 signals a change in care of address to the home agent 145 by sending a Binding Update message, secured by using an IPsec security association.

The agents 145 have a wireless access network 150 by way of which the Mobile Node 135 and Correspondent Nodes 142 communicate with the Home and Foreign Agents 145. The home agent (HA) 145 can be implemented with a router on the home link that tracks the current location of the Mobile Node 135 and relays packets to, and in some cases from, the Mobile Node 135. A home agent address (HAA) is a network address of the home agent 145.

The wireless access networks 150 may include multiple wireless access points 155. The construction, arrangement, and functionality of the wireless access networks are conventional and standard. Similarly, the implementation of wireless LAN or similar digital data communication technology in wireless, Mobile Node devices 135 and wireless access points 155 is standard. Detailed description thereof is not necessary to a complete understanding and appreciation of the present invention and is therefore omitted.

To help ensure a secure connection between the Mobile Node 135 and the Home Agents 145, a mechanism for securing telecommunication Binding Update uses Address Based Keys. Address Based Keys use long-standing results in identity based cryptosystems to construct a public key based using the IP address of the Mobile Node 135.

A security association is constructed between the Mobile Node 135 and the Home Agent 145, by using IP security protocol (IPsec) found at

ftp://ftp.isi.edu/in-notes/rfc2401.txt. The security association allows cryptographic parameter information to be distributed to the Mobile Node 135 in a confidential and authenticated fashion. The Mobile Node 135, the Home Agent 145, and Correspondent Node142 implement the identity based cryptosystem. The Home Agent 145 includes an Identity based Private Key Generator (IPKG) or includes secure access to an IPKG.

The Mobile Node 135 is preferably a node which includes an established security association with one or more Home Agents 145 on its home link. The home link includes the subnet in the Mobile Node's home network where the Mobile Node's home address is topologically located. The Mobile Node 135 can detect when it moves between different points of connection in the network 100. The Mobile Node 135 can acquire a temporary care of address in each visited location in the network 100, and signal a current care of address to the Home Agent 145 using the security association. The Correspondent Node 142 includes a node with which the Mobile Node 135 communicates. The Correspondent Node may itself be mobile. The Mobile Node 135 includes a Home Address (HoA) which can include an address of the Mobile Node 135 which does not change as the mobile node moves through the communications network 100. The Home Agent can assign the Home Address (HoA) and send the Home Address (HoA) to the Mobile Node 135.

The Home Agent 145 can be implemented with a router on the home link. The Home Agent 145 can be used to track the Mobile Node's current location and relay packets to, and in some cases from, the Mobile Node 135. To specify the Mobile Node's current location, a Care of address (CoA) IP address can be assigned to the Mobile Node 135. The Mobile Node 135 can perform Route Optimization with the Correspondent Node 142 to avoid routing packets through the Home Agent 145. Performing Route Optimization decreases the latency of communication between the Mobile Node 135 and the Correspondent Node 142. The Mobile Node 135 performs Route Optimization by sending a Binding Update to the Correspondent Node 142 when the care of address is changed. Address Based Keys (ABK) is a

technique that allows the Mobile Node 135 and Correspondent Node 142 to verify the authenticity of the Binding Updates.

The Address Based Keys (ABK) encryption technique includes an identity based cryptosystem used to generate the Mobile Node's public key from its Home Address (HoA). Other identity based cryptosystems may be used such that it allows a publicly known identifier, such as the IPv6 address, to be used as the public key for authentication, key agreement, and encryption. The Identity based Private Key Generator (IPKG) includes an agent, such as a computer processor, that can execute an identity based cryptographic algorithm to generate the private key when presented with the public identifier that will act as the public key.

Identity based cryptosystems include cryptographic techniques that allow a publicly known identifier, such as the email address or the IP address of a node, to function as the public key part of a public/private key pair for digital signature calculation, key agreement, and encryption. In identity-based signature protocols, the host, e.g. Mobile Node 135, signs a message using a private key supplied by the IPKG. The signature is then verified using the host's identity. In identity-based encryption, the encryptor uses the recipient's public identity to encrypt a message, and the recipient uses its private key to decrypt the ciphertext. As is generally the case with public key cryptography, the security of the systems depends on the difficulty of solving a hard number theory problem, such as factoring or a discrete log (or Diffie-Hellman) problem. Identity-based cryptosystems can be constructed with or without key escrow. Protocols with key escrow can be performed in fewer passes than corresponding systems that do not provide for key escrow. Techniques from threshold cryptography allow the master key information to be distributed or shared among a number of IPKGs so that all of them can collude for a host's private key to be known to them. Such a scenario would allow for key escrow if necessary, by agreement among all the IPKGs, but guards against knowledge of the private keys by the IPKGs without mutual agreement.

Identity-based cryptosystems include cryptographic systems that allow a publicly known identifier, such as an IPv6 address, to be used as a public

key for authentication, key agreement, and encryption. Address Based Keys (ABK) is a cryptographic technique where an identity-based cryptosystem is used to generate the Mobile Node's public key and private key using Public Cryptographic Parameters. Elliptic curve (EC) algorithms are preferred for identity based keys because they work well with small key sizes, are computationally efficient on small hosts, such as small wireless devices, and generate smaller signatures. Other types of algorithms such as non-EC algorithms may also be used such as by using abelian varieties in place of elliptic curves.

Public Cryptographic Parameters include a collection of publicly known parameters, specific to the identity-based cryptographic algorithm, formed from determined constants and a secret master key that is known only to the Identity -based Private Key Generator (IPKG). The IPKG includes an agent that can execute an identity-based cryptographic algorithm to generate a private key when presented with a public identifier that will act as the public key. A preferably public identifier includes the Mobile Node's Home Address (HoA). The IPKG uses a secret master key to generate the private key, and to generate the public cryptoparameters which are distributed to the Mobile Node 135 and Correspondent Nodes 142. The public cryptoparameters are used to perform cryptographic operations between two nodes involved in securing or encrypting a message, such as the Mobile Node 135 and the Correspondent Node 142.

FIG. 2 is a ladder diagram illustrating the use of an Identity-based cryptosystem to secure a Binding Update. At 200, the Mobile Node 135 submits a publicly known identifier to the Home Agent acting as IPKG 145. The publicly known identifier includes the Home Address (HoA) of the Mobile Node 135. The Mobile Node's public key is calculated by applying a hash function specific to the id cryptographic algorithm to the concatenation of the Home Address (HoA) and a determined expiration time, for example one hour. At 210, the IPKG uses an id crypographic algorithm to generate the private key and returns the private key and the expiration time to the Mobile Node 135, encrypted using the IPsec security association. The public and

private keys can then be used for authentication and encryption. Identity-based cryptographic algorithms require that a secret known only to the IPKG is used to generate the private key. As a result, unlike the Diffie-Hellman algorithm, the publicly known parameters of the cryptographic algorithm are not fixed, and therefore are not preprogrammed into the Mobile Node 135, Home Agent 145 and Correspondent Node 142. If secret master key expires or becomes compromised, the publicly known parameters are updated.

An identity-based encryption scheme includes an encryption algorithm and a decryption algorithm. Encrypted material, i.e., ciphertext, can be calculated using the following algorithm:

ciphertext = ENCRYPT(contents,IPuK,Params)

where:

ciphertext - The ciphertext.

ENCRYPT - The identity-based encryption algorithm used to encrypt the message contents.

contents - The message contents to be protected.

IPuK - The identity-based public key for the MN.

Params - The public cryptographic parameters of the IPKG.

Note that IPuK = H(ID, time), where

H - A hashing algorithm specific to the identity-based algorithm used for generating the public key from the ID.

ID - The publicly known identifier used to generate the key.

time - Simple Network Time Protocol (SNTP) Version 4 for IPv6 expiration time of the public/private key pair.

The ciphertext can be decrypted using the following algorithm:

contents = DECRYPT (ciphertext, IPrK, Params)

where:

IPrK - The identity-based private key for the mobile node.

DECRYPT - The identity-based decryption algorithm used to decrypt the ciphertext.

A message authentication code (MAC) can be calculated using the following scheme:

mac = MAC(contents, symK)

where:

mac - the computed authentication token.

MAC - the symmetric-key-based message authentication code algorithm used to compute an authentication token for a message.

contents - the message contents to be authenticated

symK - the symmetric key shared by the sender and recipient of mac.

A IPsec security association is required between the Mobile Node 135 and the Home Agent 145. The IPsec security association is used so that cryptographic parameter information and private key information can be securely distributed to the Mobile Node 135. The Mobile Node 135, Home Agent 145, and Correspondent Node 142 all implement an identity based cryptosystem. The Home Agent 145 performs as the Identity based Private Key Generator (IPKG) or has secure access to an IPKG. Initially, the Mobile Node 135 is configured to have an identity-based public/private key pair that is associated with its 128-bit IPv6 Home Address (HoA), along with the public cryptographic parameters.

At 220, after the configuration phase, the Mobile Node 135 sends a parameter retrieval initiation message to the Correspondent Node 142, such

as when the Mobile Node 135 begins a connection with a Correspondent Node 142. At 230 and 240, if the Correspondent Node 142 has not already recorded or cached the associated public cryptographic parameters, the Correspondent Node 142 securely downloads the parameters from Home Agent 145 of the Mobile Node 135. At 250, the Correspondent Node 142 then sends the Mobile Node 135 a shared secret key encrypted with Mobile Node's public key.

At 260, the Mobile Node 135 can then securely send the Binding Update. The Mobile Node 135 can send the secured Binding Update to the Correspondent Node 142 by authenticating the Binding Update with the shared secret session key. The Correspondent Node 142 can verify the authentication token by using the shared secret session key. There is no need to send the public key itself or any certificate. Also, since a symmetric key method is used to authenticate the Binding Update, there is no need to perform potentially slow public key cryptographic operations on each Binding Update. At 270, the Correspondent Node 142 can send a Binding Acknowledgement (BA) to the Mobile Node 135.

The protocol for securely distributing the private key and cryptographic parameters to the Mobile Node 135 includes the following two messages:

1) ABK Request: request private key and parameters
2) ABK Reply: return private key and parameters

The protocol for obtaining the cryptographic parameters from the HA and establishing a shared secret key using ABK includes the following four messages.

1) ABKp1: MN->CN - parameter cache directive
2) ABKp2: CN->HA - request for parameters
3) ABKp3: HA->CN - parameter return
4) ABKp4: CN->MN - parameter cache directive response

ABKp2 and ABKp3 are not necessary if the Correspondent Node 142 has cached the Home Agent 145 parameters.

Standard Mobile IPv6 Binding Update are used:.

1) BU: MN->CN - Binding Update + binding authorization data
2) BA: CN->MN - Binding Acknowledgement

These messages are described in more detail below.

The Home Agent 145 can serve as an IPKG for all Mobile Nodes within the domain of the Home Agent 145. The Home Agent 145 generates public cryptographic parameters (Params). The parameters are used with the identity-based cryptographic algorithm. The Mobile Node 135 uses the 128-bit IPv6 Home Address (HoA) assigned to the Mobile Node 135 by the Home Agent 145. The Home Address (HoA) is also used as the basis of the IPsec security association between the Home Agent 135 and the Mobile Node 135 in the base Mobile IPv6 specification.

The Mobile Node 135 then requests the private key IPrK and public cryptographic parameters from the Home Agent 145. The request can be accomplished any time prior to the Binding Update being sent, e.g., through an exchange of messages between the Home Agent 145 and the Mobile Node 135 using the pre-existing IPsec security association. The Home Agent 145 returns IPrK, the parameters, the version number of the parameters, and the SNTP time that the public/private key pair expires. The Mobile Node 135 can compute its public key as IPuK = H(HoA, expiration_time). Message formats are described below for configuring and updating the Mobile Node 135 with its ABK.

The Mobile Node 135 sends an ABKp1 message to the Correspondent Node 142 to cause the Correspondent Node 142 to initiate a request for the public cryptographic parameters. The source address of the packet is the Home Address (HoA) Mobile Node 135. ABKp1 contains a Parameters_version (Params_ver), e.g., a version number of the parameters, and a time SNTP field, e.g., an expiration time of the public/private key pair.

Upon receipt of ABKp1, the Correspondent Node 142 formulates HAA as the Mobile IPv6 Home-Agent anycast address for the subnet prefix of Home Address (HoA) of the Mobile Node 135. The Correspondent Node 142 checks for Params (of the correct version number) and the same expiration time cached for the HAA. If so, the Correspondent Node 142 does not need to send messages ABKp2 and ABKp3 and may send message ABKp4.

If the Correspondent Node 142 does not have Params of the correct version number cached or if the Correspondent Node 142 has an earlier expiration time cached, the Correspondent Node 142 sends an ABKp2 to Home Agent (HA) 145, e.g., using the destination address HAA. This assumes that valid public/private key pairs associated with a particular Home Agent (HA) 145 (PKG) include the same expiration time.

If the Correspondent Node 142 needs to send ABKp2 and ABKp3, ABKp2 contains the following fields:

HoA – the Home Address of the Mobile Node.
Nmac - Home-agent-dependent nonce MAC.

The nonce nmac is:
nmac = MAC(SHA1(HAA, N1), k_CN)

where
- N1: nonce
- k_CN: a secret key that only the CN knows

The nonce N1 is preferably refreshed periodically, but the same nonce is used for all Home Agents 145 with which the Correspondent Node 142 corresponds during the same time period. The Correspondent Node 142 can also cache recently used nonces.

Upon receipt of ABKp2, the Home Agent 145 determines whether the Home Address (HoA) of the Mobile Node 135 is a known home address. The

Home Agent (HA) 145 returns ABKp3 to Correspondent Node 142 with the following fields:

- Params.
- Params_ver: version number of the parameters
- time: SNTP expiration time of the public/private key pair.
- AF: Address change authorization flag
- nmac.

If the Home Address (HoA) is not a known home address, Params is set to NULL by the Home Agent (HA) 145. If AF is not set, then the Mobile Node 135 can use a globally unique interface identifier. The Correspondent Node 142 determines that the interface identifiers of the Home Address and the care-of address are the same. If AF is set, another method of authorizing the care-of address to change the routing could be used. Upon receipt of ABKp3, the Correspondent Node 142 checks Params and computes MAC(SHA1(HAA, N1), k_CN). If Params is set to NULL or if nmac does not match the computed MAC value then authenticatoin fails. The Correspondent Node 142 does not send an error message. If Params is not NULL, the Correspondent Node 142 caches HAA (source address of message ABKp3), the parameters, the version number of the parameters, the current key expiration time, and the address change authorization flag.

ABKp4 contains the following field:

E = ENCRYPT(k_m, IPuK, Params)

where

k_m = SHA1(HoA, k_CN).

k_m is a secret key that the Correspondent Node 142 generates and shares with the Mobile Node 135. The key is encrypted with the public key

IPuK of the Mobile Node 135, which may be derived from the Home Address (HoA) of the Mobile Node 135 and the public/private key expiration time. When the Mobile Node 135 receives ABKp4, it computes k_m = DECRYPT(E, IPrK, Params) to use in computing the Binding Update.

A Binding Update message can be sent from the Mobile Node 135 to the Correspondent Node 142 according to standard Mobile IPv6 procedures. In addition to the standard fields, the Binding Update contains a Binding Authorization Data option, which contains a MAC calculated over the following fields:

The BU contents (including HoA).
k_r - random value generated by the Mobile Node.

The Authenticator calculated as follows:

mac = MAC(SHA1(BU, k_r), k)

where the session key can be computed as k = SHA1(k_m | k_r).

Upon receiving the Binding Update, if the address change authorization flag AF is not set for the Home Address (HoA) of the Mobile Node 135, the Correspondent Node 142 determines whether the interface identifier on the proposed Care of Address (CoA) matches the interface identifier on the Home Address (HoA) in the Home Address Option of the Binding Update packet. If the interface identifier does not, the Correspondent Node 142 sends a Binding Acknowledgment (BA) with the appropriate error code.

If AF is set, then the Binding Update begins an address change authorization algorithm to determine whether the Mobile Node 135 can change the address.

If AF is not set and the interface identifier on the proposed Care of Address (CoA) matches that of the Home Address (HoA) in the Home Address Option of the Binding Update packet or if the AF is set and the

address change is authorized, the Correspondent Node 142 computes k_m = SHA1(HoA, k_CN) and then computes k = SHA1(k_m | k_r). The Correspondent Node 142 then verifies the Binding Update by comparing the value mac from the Authenticator in the Binding Authorization Data option to MAC(SHA1(BU, k_r), k). If the two values match, the Correspondent Node 142 sends a Binding Acknowledgment (BA) message that indicates success; otherwise, the Correspondent Node 142 sends a Binding Acknowledgment (BA) message that indicates failure.

The Mobile Node 135 uses the same interface identifier for its Care of Address (CoA) as in the Home Address (HoA), unless the Home Agent (HA) 145 has indicated otherwise in ABKp3 by setting the Address Change Authorization flag. If the flag is not set and a different interface identifier appears in the binding update, the Correspondent Node 142 rejects the Binding Update and sends an error Binding Acknowledgment (BA) to the Mobile Node 135 that indicates that the Binding Update is rejected.

The Mobile Node 135 may use a different interface identifier for the Care of Address (CoA) if the Home Agent 145 has indicated by setting the Address Change Authorization flag that some procedure is in place. The different interface identifier allows the Correspondent Node 142 and Mobile Node 135 to agree on a way of authorizing that a Mobile Node 135 with a particular Home Address (HoA) is allowed to change to a particular Care of Address (CoA). Cryptographically generated addresses and AAA are examples of such procedures.

The Mobile Node/Home Address (HoA) association can be verified. The Correspondent Node 142 receives parameters directly from the Home Agent (HA) 145. Also, only the true Mobile Node 135 can decrypt the shared secret key, which is used to generate the session keys that authenticate the Binding Updates.

If a Mobile Node 135 attempts to flood a Correspondent Node 142 with ABKp1 messages, for each message, the Correspondent Node 142 checks a parameters table to determine if the Correspondent Node 142 has the parameters for the relevant Home Agent 145. If not, the Correspondent Node

142 sends an ABKp2 message to the Home Agent 145 to request parameters. The Correspondent Node 142 will not send an ABKp2 message to the same Home Agent 145 more than once unless the parameters have expired. The Correspondent Node 142 does not create state. If a Home Agent 145 is flooded with ABKp2 messages, the Home Agent 145 discards all messages that include a Home Address (HoA) that is not in the domain of the Home Agent 145.

The nonce MAC nmac is used to prevent attackers who might attempt to initiate communications with the Correspondent Node 142, or flood the Correspondent Node 142 by using message ABKp3. For a flood of ABKp4 messages, the Mobile Node 135 ignores any messages if the Mobile Node 135 did not initiate an ABKp1 message. The Correspondent Node ignores Binding Update messages whose MACs cannot be verified. The Mobile Node 135 ignores Binding Acknowledgment (BA) messages from nodes with which Mobile Node 135 did not initiate a Binding Update.

If an attacker on one path between any two entities (Mobile Node 135, Correspondent Node 142, Home Agent 145) can alter messages, at worst the Binding Update would fail. The Correspondent Node 142 could continue to send Mobile Node packets to an old Care of Address (CoA). Since messages ABKp1 through ABKp3 are not signed, a possibility exists to change them. However, if message ABKp4 is encrypted in a way that ABKp4 can also be authenticated, ABKp4 cannot be changed. The Binding Update is accomplished with MAC, so that the Binding Update is not susceptible to a data alteration attack.

Alternatively, if the Correspondent Node 142 includes a standard public key certificate for the Home Agent 145, the Correspondent Node 142 can use another protocol, such as a TLS (Transport Level Security, RFC 2246) protocol to transact ABKp2 through ABKp3. The TLS protocol can prevent an attack on the Home Agent transaction.

A redirect attack can occur if the Mobile Node 135 can send the Correspondent Node 142 a Binding Update containing an false Care of Address (CoA) in a different subnet that corresponds to the victim. The

Correspondent Node 142 will then redirect the Mobile Node's traffic to the victim, even though the victim has no interest in the traffic. Redirect attacks can be prevented by requiring that the Mobile Node 135 use an interface identifier assigned to it by the Home Agent 145 in the Home Address (HoA) of the Mobile Node 135 to also form the Care of Address (CoA). This prevents the Mobile Node 135 from forming a Care of Address (CoA) that corresponds to any node other than itself. The Mobile Node 134 uses the same interface identifier in every Care of Address (CoA). Use of the same identifier does not limit route optimization because route optimized packets contain a Home Address Option containing the home address anyway.

An ABK distribution protocol provides the Mobile Node 135 with an ABK from the Home Agent 145 initially and periodically if necessary when the key expires or if the parameters change. The protocol uses TCP (Transmission Control Protocol) transport to a port to be assigned, for example, by IANA. The protocol can be secured using IPsec ESP and the Home Agent/Mobile Node security association defined by the base Mobile IPv6 specification. The protocol contains two messages, an ABK Request and an ABK Reply.

FIG. 3 illustrates an ABK Request message. The ABK Request message is sent by the Mobile Node 135 to the Home Agent 145 to request a new ABK. The source address is the Mobile Node home address. The destination address is the Home Agent address. An IPsec Header such as an ESP IPsec header for the Home Agent/Mobile Node security association can be included, and the packet can be encrypted using the shared key. The ABK message type code 300 is set to an identifier, such as 5. The #Alg. Ids 310 is the number of four byte algorithm identifier records to follow, which is not zero. For each record, the Alg. Id 320 includes a two byte identity-based cryptographic algorithm identifier, assigned by IANA. Params_ver 330 includes a two byte parameter version number for the algorithm identifier.

If the Mobile Node 135 is not on the home network, the Mobile Node 135 establishes a valid binding between the Care of Address (CoA) and Home Address (HoA) before sending this message and reverse tunnel the

message to the Home Agent 145 to avoid ingress filtering on the foreign subnet. The Mobile Node 135 includes a list of identity-based cryptographic algorithm identifiers indicating the algorithms that the Mobile Node 135 supports, and the version numbers for the latest version of the parameters known to the Mobile Node 135. The list may be in order of the Mobile Node preferences, for example, with the most preferred algorithm first.

The IPsec security association assures that only Mobile Nodes 135 with valid, assigned Home Addresses (HoAs) can communicate with the Home Agent 145. Upon receipt of an ABK Request, for each algorithm in the list in which the parameter version is not equal to the most current version, the Home Agent 145 calculates IPrK. First, the Home Agent 145 calculates IPuK using the source address of the packet, e.g., the Home Address (HoA) as the public identifier, and an SNTP expiration time for the key. Next, the Home Agent 145 uses IPuK, the parameters, and the algorithm to calculate IPrK. The results are returned to the Mobile Node 134 in the ABK Reply message.

FIG. 4 illustrates an ABK Reply message. The ABK Reply message contains a list of parameters for the algorithms requested by the Mobile Node 135 and supported by the Home Agent 145. An expiration time value also is included, which the Mobile Node 135 used to compute the public key. Regarding the IP fields, the Source Address is the Home Agent address. The Destination Address is the Home Address (HoA) of the Mobile Node. Regarding IP Headers, the ESP IPsec header for the Home Agent/Mobile Node security association is included, and the packet is encrypted using the shared key.

Regarding the Message Fields, the ABK message type code 400 is set to a number, such as 6, that differentiates the message from other messages. The Key Expiration Time 410 includes a four byte positive integer giving the time that the key expires. The #Param/Key Recs 420 includes the number of per algorithm variable length records including parameters and keys to follow. For each record, the Length of Param/Key Rec. 430 is the Length, in bytes, of the parameter record to follow, including the Alg. Id. 440, Params_ver 450, and Parameters + IPrK list 460. The Alg. Id 440 is a two byte identity-based

cryptographic algorithm identifier, assigned by IANA. The Params_ver 450 is a two byte parameter version number for the algorithm identifier. The Parameters + IPrK 460 is a variable length parameters + IPrK list, the format of which is specified by the algorithm identifier specification.

The Home Agent 145 returns an ABK Reply message in response to an ABK Request, encrypted and with the proper ESP security header. The ABK Reply message can be tunneled to the Mobile Node 135 at its CoA if the Mobile Node 1353 is not in a home network, just as with other traffic routed through the Home Address (HoA) of the Mobile Node 135. If the Home Agent 145 does not support any of the algorithms requested by the Mobile Node 135, the Key Expiration time 410 and #Param Recs 420 fields are zero. Otherwise, these fields are other than zero. If the Home Agent 145 does not support a particular algorithm, a record can be included with the indicated algorithm's Alg. Id 440. If the algorithm is not supported, the Params_ver 450 field is zero and no Parameters + IPrK field 460 is used.

If the parameter version in the ABK Request for a particular algorithm supported by the Mobile Node 135 is current, a record can be included with the indicated algorithm's Alg. Id 440 and the current Params_ver 450, but no Parameters + IPrK field 460 is needed. The Mobile Node 135 can continue to use cached parameters and IPrK until the parameters change or its key expires. The IPsec security association assures that the Home Agent 145 can send the Mobile Node 135 an ABK Reply. Upon receipt of the ABK Reply, the Mobile Node caches the IPrKs and parameters for each algorithm, for use in securing Binding Updates. When the keys expire, the Mobile Node 135 requests a new private key IPrK for the identity-based cryptographic algorithms that the Mobile Node 135 supports.

During the parameter initialization phase, the Mobile Node 135 requests that the Correspondent Node 142 initialize the parameters from the Home Agent 145. The Mobile Node 135 operates the parameter initialization protocol when the Mobile Node 135 changes IPrK and parameters. The protocol uses TCP over the IANA TBD assigned port as used for the ABK distribution protocol. The Mobile Node 135 can reverse tunnel ABKp1

through the Home Agent 145 to the Correspondent Node 142, if not located on the home network, to initiate the protocol. ABKp4 can be tunneled through the Home Agent 145 to the Mobile Node 142 by standard Mobile IP mechanisms. ABKp2 and ABKp3 are exchanged between the Correspondent Node 142 and Home Agent 145.

FIG. 5 illustrates an ABKp1 message. ABKp1 is reverse tunneled from Mobile Node 135 through the Home Agent 145, if the Mobile Node 135 is not located on the home network, to the Correspondent Node 142 to being the protocol for securing a Binding Update. The source address is the Home Address of the Mobile Node 135. The destination address is the address of the Correspondent Node 142. The ABK message type code 500 is set to a number to differentiate from other messages, such as 1. The #Alg. Ids 510 is the number of four byte algorithm identifier records 520 to follow, greater than zero. For each record, the Alg. Id 520 is a two byte identity-based cryptographic algorithm identifier, assigned by IANA. The Params_ver 530 is a two byte parameter version number for the algorithm identifier. The parameter version number identifies the version of the parameters currently held by the Mobile Node 135. The Key Expiration Time 540 is a four-byte SNTP time which identifies the expiration time of the Mobile Node's key.

FIG. 6 illustrates an ABKp2 message. ABKp2 is sent by the Correspondent Node 142 to the Home Agent 145. The source address is the address of the Correspondent Node 142. The destination address is the Home Agent anycast address located in the Mobile Node's subnet, determined by the Home Address (HoA) subnet prefix of the Mobile Node 135. The Message Fields include a Type field 600. The ABK message type code is set to a number different from other messages, such as 2. The Reserved field 610 is set to zero upon transmission and ignored on reception. The nmac field 620 identifies nonce MAC, a 160 bit HMAC SHA-1 value. The HoA field 630 identifies the Home Address of the Mobile Node 135. The #Alg. Ids field 640 identifies the number of two byte algorithm identifier records to follow, which is not zero. For each record, Alg. Id 650 identifies a two byte identity-based cryptographic algorithm, assigned by IANA or another entity.

The algorithm id list identifies the algorithms supported by the Correspondent Node 142 that were included in the list sent by the Mobile Node 135 in ABKp1, for which the version number of the parameters cached by the Correspondent Node 142 does not match that sent by the Mobile Node 135. The Correspondent Node 142 does not send ABKp2 if the Correspondent Node 142 has a set of cached parameters with a version number matching at least one of the algorithms on the list sent by the Mobile Node 135 in ABKp1. The Correspondent Node 142 uses the matching algorithm.

FIG. 7 illustrates an ABKp3 message. The source address is the address of the Home Agent 145. The destination address is the address of the Correspondent Node 142. The Message Fields include a Type field 700. The ABK message type code is set to a unique message number, such as 3. The A field identifies an Unset and Set command. The Unset command is used if the Home Agent 145 requires the Mobile Node 135 to use the same interface identifier for CoAs as for the Home Address (HoA). The Set command is used if a different address change authorization procedure is used. The Reserved field 720 is set to zero upon transmission. The nmac field 730 identifies nonce MAC, a 160 bit HMAC SHA-1 value that matches the nonce value sent in ABKp2.

The #Param Recs 740 identifies the number of variable length parameter records to follow. For each record, the Length of Param Rec field 750 identifies the length, e.g., in bytes, of the parameter record to follow, including the Alg. Id. 760, the Params_ver 770, and the Parameters 780. The Alg. Id field 760 includes a two byte identity-based cryptographic algorithm identifier, e.g., assigned by IANA. The Params_ver field 770 includes a two byte parameter version number for the algorithm identifier. The Parameters field 780 includes a variable length parameters list 790, the format of which can be determined by the algorithm identifier specification.

If the Home Agent 145 has no record of the Home Address (HoA) of the Mobile Node 135, the Home Agent 145 returns ABKp3 with the #Param Recs. field 740 set to zero. Otherwise, #Param Recs. field 740 is not set to

zero. If the Home Agent 145 does not support one of the algorithms on the list sent in ABKp3, the Home Agent 145 sends a record with the indicated algorithm's identifier in the Alg. Id field 760, the Params_ver field 770 is set to zero and no parameters exist in the Parameters field 780. Otherwise, the Home Agent 145 includes a parameter record for each algorithm included in ABKp2 for which the Home Agent 145 has parameters.

FIG. 8 illustrates an ABKp4 message. Regarding the IP Fields, the Source Address is the Correspondent Node's address. The Destination Address is the home address of the Mobile Node. The Message Fields include the Type field 800. The ABK message Type field 800 code is set to a unique message number, such as 4. A Status Code field 810 includes a code indicating a message status. Exemplary recognized codes follow:

0 - Status OK.

1 - No algorithm supported. A '1' code is returned if the Mobile Node 135 and the Correspondent Node 142 do not share an algorithm in common.

2 - Parameters out of date. A '2' code is returned if the version numbers of the parameters returned by the Home Agent 142 for all algorithms shared with the MN are newer than the version numbers provided by the Mobile Node 135.

The Alg. Id field 820 is a two byte algorithm identifier for the algorithm to be used by the Correspondent Node 142 to encrypt the Session Key. The Length of Encrypted Key field 830 identifies the length, in bytes, of the encrypted session key (E). As described above, E can equal ENCRYPT(k_m, IPuK, Params). The Encrypted Session Key (E) is contained in the 'E' field 840.

The algorithm identifier specification contains the format of the shared key and other data. The Correspondent Node 142 selects an algorithm from the list sent by the Mobile Node 135 in ABKp1 for which parameters are

available as returned by the Home Agent 145 in ABKp3, or cached by the Correspondent Node 142 if no ABKp2/ABKp3 message was necessary. The Correspondent Node 142 includes the selected algorithm's identifier in the Alg. Id field 820. The Correspondent Node 142 can select the algorithm closest to the beginning of the list sent by the Mobile Node 142 in ABKp1, since the list is sorted by order of Mobile Node preference.

The Encrypted Session Key field 840 contains the session key, encrypted using the public key (calculated from the home address (HoA) of the Mobile Node 135 and the key expiration time) and the algorithm parameters. The format of this field depends on the algorithm and is included in the algorithm specification. The Correspondent Node 142 does not send a return message if the Home Agent 145 indicates that the Home Agent 145 does not recognize the Mobile Node's Home Address (HoA).

If the Correspondent Node 142 is able to select an algorithm with parameters on which the Correspondent Node 142 and Mobile Node 135 agree, the Status Code field 810 is set to zero and the remainder of the message is filled. If the Status Code field is not zero, the Correspondent Node 142 does not include any other fields. If the Correspondent Node 142 and Mobile Node 135 can agree on at least one algorithm and the parameter versions match, the Correspondent Node 142 selects that algorithm. The Correspondent Node 142 does not send a nonzero status code unless there are no matching choices.

A Mobile Node 135 using ABK to secure Binding Updates includes a standard Mobile IPv6 Binding Authorization Data extension, with the authentication token _mac_, calculated as described above, in the Authenticator field. The Correspondent Node 142 verifies the Authenticator, as described above. If the Authenticator fails to be verified, the Correspondent Node 142 returns a Binding Acknowledgement (BA) with error code 137, Invalid authenticator. If the address change authorization check fails, an error code is sent that the Mobile Node 135 is not authorized for that CoA.

For an identity-based encryption algorithm to be used in ABK Binding Updates, a specification exists to describe the algorithm and provide, an IANA assigned algorithm type code, a format of the Parameters + IPrK field in the ABK Reply message, a format of the Parameters field in ABKp3, and a format of E in ABKp4. The specification is established by IETF standards action. A TCP socket number is determined for the protocol, to be assigned by IANA. A Mobile IP Binding Acknowledgement error code may be determined for when the Mobile Node 135 is not authorized to change to a particular Care of Address CoA.

While the invention has been described above by reference to various embodiments, it will be understood that many changes and modifications can be made without departing from the scope of the invention. It is therefore intended that the foregoing detailed description be understood as an illustration of the presently preferred embodiments of the invention, and not as a definition of the invention. It is only the following claims, including all equivalents, which are intended to define the scope of this invention.

CLAIMS

1. A method of securing binding updates in a wireless telecommunications system, the method comprising:

generating a public key using a publicly known identifier;

generating a private key using the public key; and

utilizing the public key and the private key to secure binding updates.

2. The method of claim 1 wherein a home agent generates the public key.

3. The method of claim 1 wherein a home agent generates the private key.

4. The method of claim 3 wherein the home agent provides the private key to the mobile host.

5. The method of claim 4 further including a correspondent node connectable with a mobile host, wherein the public key, a shared key and a public parameter are used to secure binding updates between the mobile host and the correspondent node.

6. The method of claim 5 wherein the correspondent node encrypts the shared key with the public key and the public parameter.

7. The method of claim 5 wherein the mobile host uses the shared key to sign the binding update and sends a signed binding update to the correspondent node.

8. The method of claim 5 wherein the home agent provides the public parameters to the correspondent node.

9. The method of claim 1 wherein the public key is generated using a home address value of the mobile host.

10. A system for securing binding updates in a wireless telecommunications system, comprising:

a mobile host connectable to the telecommunications system;

a correspondent node connectable with the mobile host, wherein a public key and a private key are used to secure binding updates between the mobile host and the correspondent node.

11. The system of claim 10 further including a home agent connectable with the mobile host and correspondent node.

12. The system of claim 11 wherein the home agent generates the private key and a public parameter.

13. The system of claim 10 wherein the public key is generated using a home address value of the mobile host.

14. The system of claim 11 wherein the home agent generates the private key.

15. The system of claim 11 wherein the home agent provides the private key and public parameters to the mobile host.

16. The system of claim 15 wherein a correspondent node encrypts a shared key with the public key and public parameters.

17. The system of claim 16 wherein the mobile host uses the shared key to sign the binding update and sends a signed binding update to the correspondent node.

18. The system of claim 16 wherein the mobile host provides the public parameters to the correspondent node.

19. A mobile node for use in a wireless telecommunications system, comprising:

an interface capable of connecting the mobile node to a home agent and a corresponding node, wherein a public key and a private key are

used to secure binding updates between the mobile node and the correspondent node.

20. The mobile node of claim 19 wherein the home agent generates the private key and a public parameter.

21. The mobile node of claim 19 wherein the public key is generated using a home address value of the mobile node.

22. The mobile node of claim 19 wherein the home agent generates the private key.

23. The mobile node of claim 19 wherein the home agent provides the private key and public parameters to the mobile node.

24. The mobile node of claim 23 wherein the correspondent node encrypts a shared key with the public key and public parameters.

25. The mobile node of claim 24 wherein the mobile node uses the shared key to sign the binding update and sends a signed binding update to the correspondent node.

26. The mobile node of claim 24 wherein the interface is used to provide the public parameters to the correspondent node.

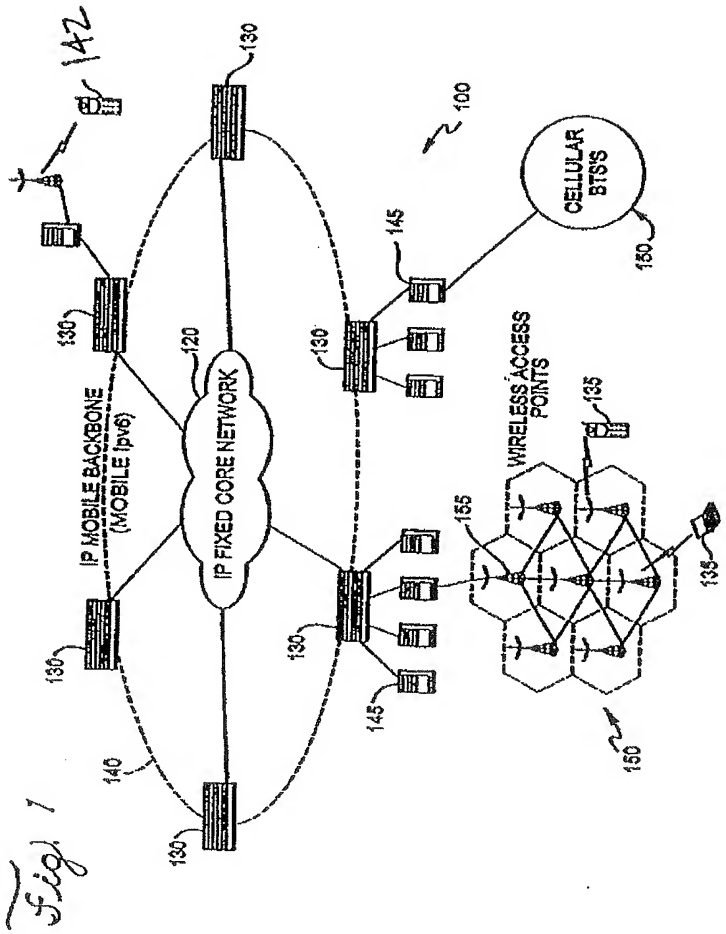

142
130
100
CELLULAR BTS'S
150
145
IP MOBILE BACKBONE (MOBILE Ipv6)
120
IP FIXED CORE NETWORK
WIRELESS ACCESS POINTS
135
155
140

Fig. 1

2/8

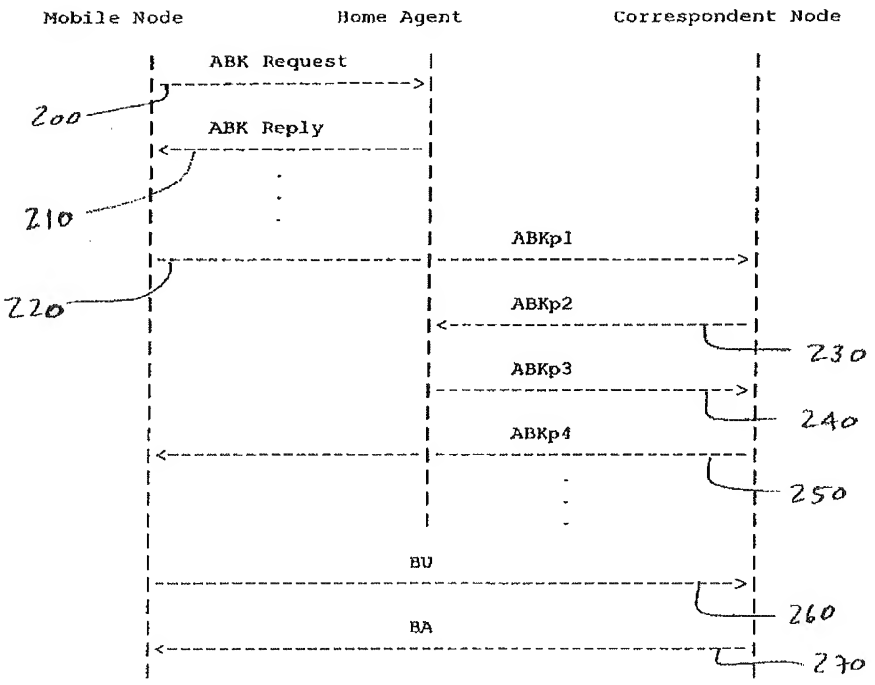


Fig. 2

3/8

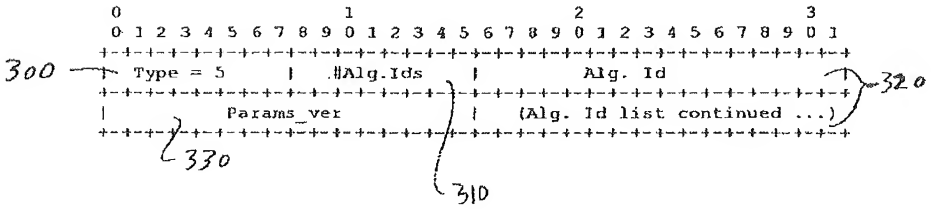


FIG. 3

4/8

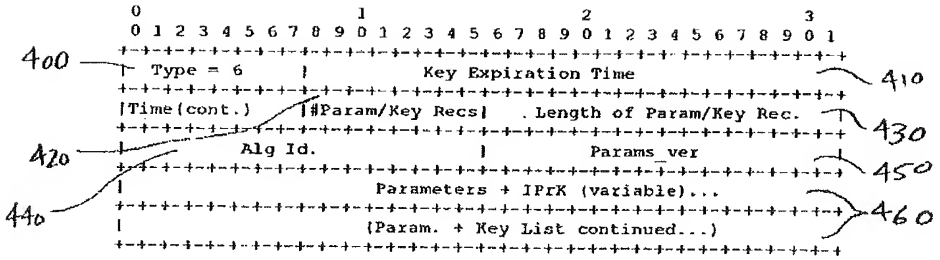


FIG. 4

5/8

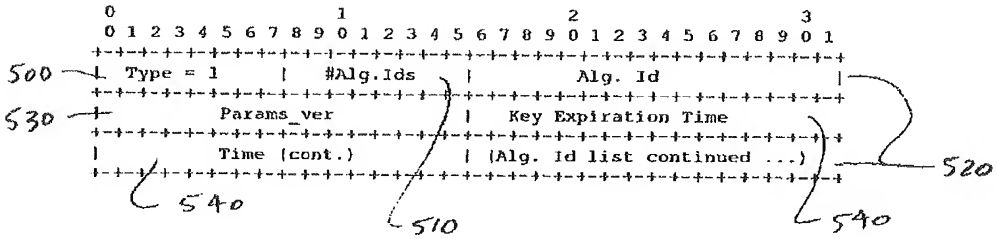


FIG. 5

6/8

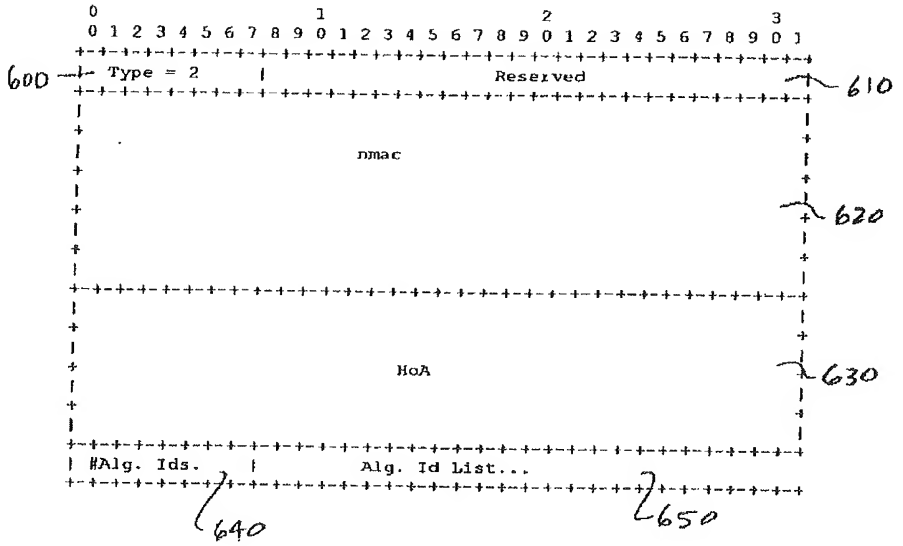


FIG. 6

7/8

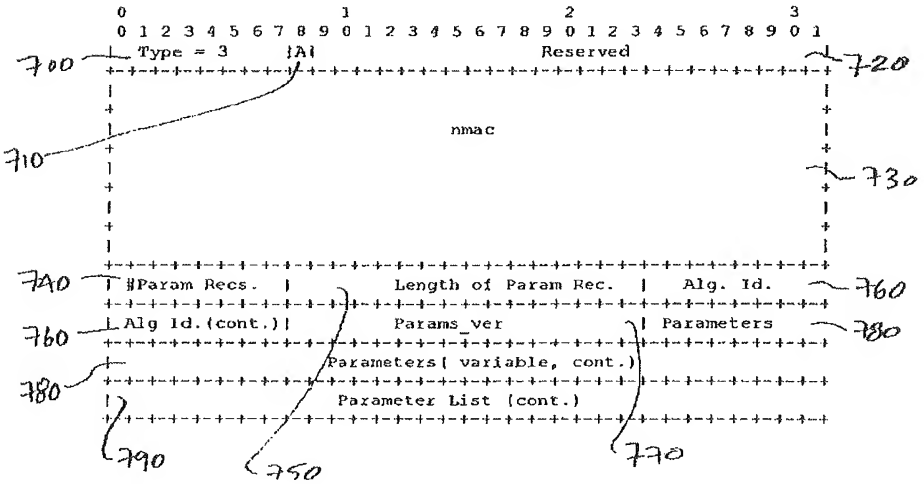


FIG. 7

8/8

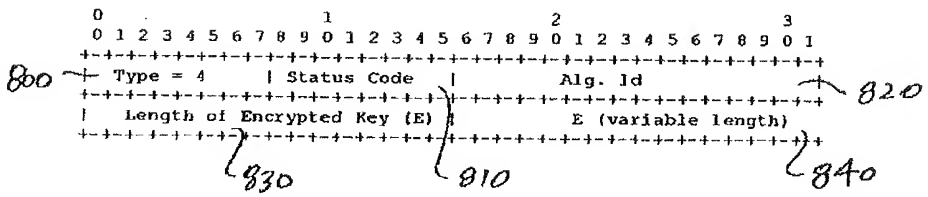

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type = 4
Status Code
Alg. Id
Length of Encrypted Key (E)
E (variable length)
800
820
830
810
840

FIG. 8

ABSTRACT

A system and method are disclosed for securing binding updates in a wireless telecommunications system. A public key is generating using a home address value of the mobile host. Thereafter, a home agent, such as a router, generates a private key using public cryptographic parameters, that corresponds to the mobile host and the public key. The correspondent node uses the public key to encrypt a shared key and sends the shared key to the mobile host. The mobile host decrypts the shared key using the private key and uses the shared key to sign the binding update. Thereafter, the correspondent node utilizes the shared key to verify the authenticity of the binding update.